Novell
Identity Manager

3.0

www.novell.com

2005 年 12 月 8 日

IDENTITY MANAGER 用户应用程序：管理指南

Novell

法律声明

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

联机文档：要访问本产品和其它 Novell 产品的联机文档并获取产品的更新资料，请参见 www.novell.com/documentation。

Novell 商标

第三方材料

所有第三方商标是其各自拥有者的资产。

第三方法律声明

Apache 软件许可证 *1.1* 版

版权所有 (c) 2000 The Apache Software Foundation。保留所有权利。

本软件允许在修改或不修改的情况下以源代码和二进制形式进行再分发和使用，前提是遵守以下条件：

1. 如果以源代码形式再分发，则必须在源代码中保留上述版权声明、本条件列表和以下免责声明。
2. 如果以二进制形式再分发，则必须在随分发提供的文档和 / 或其它材料中复制上述版权声明、本条件列表和以下免责声明。
3. 再分发中包括的终端用户文档 （如果有）必须包含以下鸣谢：《本产品包含由 Apache Software Foundation (http://www.apache.org/) 开发的软件。》

或者，在软件本身中通常出现此类第三方鸣谢的地方，显示本鸣谢。

4. 未经事先书面许可，不得使用名称 《Apache》和 《Apache Software Foundation》来签署或宣传从本软件衍生的产品。有关书面许可，请联系 apache@apache.org。
5. 未经 Apache Software Foundation 事先书面许可，不得将本软件的衍生产品命名为 《Apache》或在其名称中包括 《Apache》。

本软件 《按原样》提供，并且不做任何明示或暗示保证，包括但不限于对用于任何具体目的的适销性或适用性的暗示保证。在任何情况下，对于因使用本软件而产生的任何直接、间接、意外、特殊、典型或因果性损害 （包括但不限于替代商品或服务的获得；使用、数据或利润丧失；或业务中断），无论出于何种起因，也无论根据何种责任 （无论合同中是否规定）、严格责任或其它责任理论 （包括疏忽或其它原因）， Apache Software Foundation 或其供应者均不负责。即使被告知这种损害的可能性时，也是如此。

Autonomy

版权所有 ©1996-2000 Autonomy, Inc.

Bouncy Castle

许可版权 (c) 2000 - 2004 The Legion Of The Bouncy Castle (http://www.bouncycastle.org)

对于获取了本软件及其关联的文档文件 （统称 《软件》）的任何人员，本许可在此免费授予其不受限制地经营本软件的权利，包括但不限于使用、复制、修改、合并、发布、分发、转发许可证和 / 或出售软件副本的权利。在本软件向上述人员提供这些权利时，必须满足以下条件：

本软件的所有副本或重要部分中均包含上述版权声明和此许可声明。

本软件 《按原样》提供，并且不做任何明示或暗示保证，包括但不限于用于任何具体目的的适销性、适用性保证和非侵权性保证。在任何情况下，对于因本软件或对本软件的使用或其它处理而引起的任何索赔、损害或其它责任，无论该行为是否符合合同的规定，作者或版权所有者均不负责。

Castor Library

原始许可证位于 http://www.castor.org/license.html 上

此项目的代码在类似 BSD 的许可证 [license.txt] 下发行：

版权所有 1999-2004 (C) Intalio Inc. 及其它。保留所有权利。

本软件及相关文档 （统称 《软件》）允许在修改或不修改的情况下进行再分发和使用，前提是遵守以下条件：

1. 如果以源代码形式再分发，则必须在源代码中保留版权声明。再分发还必须包含此文档的副本。
2. 如果以二进制形式再分发，则必须在随分发提供的文档和 / 或其它材料中复制上述版权声明、本条件列表和以下免责声明。
3. 未经 Intalio Inc. 事先书面许可，不得使用名称 《ExoLab》来签署或宣传从本软件衍生的产品。有关书面许可，请联系 info@exolab.org。
4. 未经 Intalio Inc. 事先书面许可，不得将本软件的衍生产品命名为 《Castor》或在其名称中包括

《Castor》。 Exolab、 Castor 和 Intalio 均为 Intalio Inc. 的商标。

5. ExoLab? Project (http://www.exolab.org/) 享有预期的权益。

本软件由 INTALIO 及供应者 《按原样》提供，并且不做任何明示或暗示保证，包括但不限于对用于任何具体目的的适销性或适用性的暗示保证。在任何情况下，对于因使用本软件而产生的任何直接、间接、意外、特殊、典型或因果性损害 （包括但不限于替代商品或服务的获得；使用、数据或利润丧失；或业务中断），无论出于何种起因，也无论根据何种责任 （无论合同中是否规定）、严格责任或其它责任理论 （包括疏忽或其它原因）， INTALIO 或其供应者均不负责。即使被告知这种损害的可能性时，也是如此。

Indiana University Extreme! Lab 软件许可证

版本 1.1.1

版权所有 (c) 2002 Extreme! Lab， Indiana University。保留所有权利。

本软件允许在修改或不修改的情况下以源代码和二进制形式进行再分发和使用，前提是遵守以下条件：

1. 如果以源代码形式再分发，则必须在源代码中保留上述版权声明、本条件列表和以下免责声明。
2. 如果以二进制形式再分发，则必须在随分发提供的文档和 / 或其它材料中复制上述版权声明、本条件列表和以下免责声明。
3. 再分发中包括的终端用户文档 （如果有）必须包含以下鸣谢： 《本产品包含由 Indiana University Extreme! Lab (http://www.extreme.indiana.edu/) 开发的软件。》

或者，在软件本身中通常出现此类第三方鸣谢的地方，显示本鸣谢。

4. 未经事先书面许可，不得使用名称 《Indiana University》和 《Indiana University Extreme! Lab》来签署宣传从本软件衍生的产品。有关书面许可，请联系 http://www.extreme.indiana.edu/。
5. 未经 Indiana University 事先书面许可，不得将本软件的衍生产品命名为 《Indiana University》或在其名称中包括 《Indiana University》。

本软件 《按原样》提供，并且不做任何明示或暗示保证，包括但不限于对用于任何具体目的的适销性或适用性的暗示保证。在任何情况下，对于因使用本软件而产生的任何直接、间接、意外、特殊、典型或因果性损害 （包括但不限于替代商品或服务的获得；使用、数据或利润丧失；或业务中断），无论出于何种起因，也无论根据何种责任 （无论合同中是否规定）、严格责任或其它责任理论 （包括疏忽或其它原因），作者、版权所有者或其供应者均不负责。即使被告知这种损害的可能性时，也是如此。

JDOM.JAR

版权所有 (C) 2000-2002 Brett McLaughlin & Jason Hunter。保留所有权利。

本软件允许在修改或不修改的情况下以源代码和二进制形式进行再分发和使用，前提是遵守以下条件：

1. 如果以源代码形式再分发，则必须在源代码中保留上述版权声明、本条件列表和以下免责声明。
2. 如果以二进制形式再分发，则必须在随分发提供的文档和 / 或其它材料中复制上述版权声明、本条件列表和以下免责声明。
3. 未经事先书面许可，不得使用名称 《JDOM》来签署或宣传从本软件衍生的产品。有关书面许可，请联系 license@jdom.org。
4. 未经 JDOM Project Management (pm@jdom.org) 事先书面许可，不得将本软件的衍生产品命名为 《JDOM》或在其名称中包括 《JDOM》。

另外，我们希望 （但不要求）您在随再分发和 / 或软件自身提供的终端用户文档中包含以下类似鸣谢：《本产品包含由 JDOM Project (http://www.jdom.org/) 开发的软件。》

或者，此类鸣谢可采用 http://www.jdom.org/images/logos 中提供的徽标以图形方式显示。

本软件 《按原样》提供，并且不做任何明示或暗示保证，包括但不限于对用于任何具体目的的适销性或适用性的暗示保证。在任何情况下，对于因使用本软件而产生的任何直接、间接、意外、特殊、典型或因果性损害 （包括但不限于替代商品或服务的获得；使用、数据或利润丧失；或业务中断），无论出于何种起因，也无论根据何种责任 （无论合同中是否规定）、严格责任或其它责任理论 （包括疏忽或其它原因）， JDOM 作者或项目供应者均不负责。即使被告知这种损害的可能性时，也是如此。

Phaos

W3C

W3C® 软件声明和许可

目录

关于本书

用途

本书介绍如何管理 Novell Identity Manager 用户应用程序，包括：

- 随 Identity Manager 提供的身份自助服务功能
- 基于工作流程的供应功能，前提是您为 Identity Manager 添加了预置模块

要了解有关如何管理 Identity Manager 的其它功能 （对所有包都相同）的信息，请参见《*Novell Identity Manager*：管理指南》。

读者

本书中的信息面向负责对 Identity Manager 用户应用程序的身份自助服务功能和 / 或基于工作流程的供应功能进行配置、部署和管理的系统管理员、设计者和顾问。

有关这些功能的终端用户文档，请参见 《*Identity Manager* 用户应用程序：用户指南》。

前提条件

本书假设：

- 您已经安装了 Identity Manager，并且可能也安装了 Identity Manager 的预置模块

有关安装这些产品的说明，请参见 《*Novell Identity Manager*：安装指南》。

- 您已经配置了符合您需要的其它 Identity Manager 功能

请参见 《*Novell Identity Manager*：管理指南》。

组织

下面是本书的摘要：

部分	说明
"概述" 在第 11 页	介绍 Identity Manager 用户应用程序，并帮助您计划如何在组织中使用它
"配置用户应用程序环境" 在第 47 页	如何配置 Identity Manager 用户应用程序环境的各个方面 （包括用户应用程序驱动程序、目录提取层和日志记录）以满足组织的需要
"管理用户应用程序" 在第 117 页	如何使用用户界面的 《管理》选项卡配置和管理 Identity Manager 用户应用程序
"入口小程序参照" 在第 215 页	如何配置 Identity Manager 用户界面中使用的身份和系统入口小程序

部分	说明
“设计和管理供应请求”在第 281 页	如何使用 Identity Manager 的预置模块配置、部署和管理供应所需的资源、工作流程和请求定义 **注释：**仅当具有 Identity Manager 预置模块时，此部分才适用。
“附录”在第 333 页	Identity Manager 用户应用程序的附加参考信息 （纲要扩展）和高级主题 （配置应用程序存档）

另请参见

有关其它相关的手册和自述信息，请转至 Novell 文档万维网站点的 《Identity Manager》页 (http://www.novell.com/idm/)。

概述

这些章节将向您介绍 Identity Manager 用户应用程序，并帮助您计划如何在组织中使用它。

概述 1

Novell Identity Manager 用户应用程序是一款强大的万维网应用程序，专门用于在复杂的身份服务框架上提供丰富、直观、可配置性和可管理性强的用户体验。当 Identity Manager 用户应用程序与 Identity Manager 预置模块和 Novell Audit 一起使用时，它可以提供一个完整的、端对端的供应解决方案，具有安全、可伸缩、易于管理的特点。

用户应用程序提供以下基于万维网的终端用户功能：

- 白页
- 组织图
- 用户搜索 （具有保存自定义搜索配置的功能）
- 自助服务口令管理
- 轻量级用户管理工具
- 工作流程的启动和监视 （如果已安装预置模块）
- 管理个人和 / 或小组任务 （如果已安装预置模块）
- 委托和代理功能

此用户应用程序可为系统管理员提供多种配置和管理功能，包括：

- 允许设置和管理代理及委托权限的界面
- 对日志记录工具和自定义 Crystal Reports 的访问
- 基于向导的工作流程配置 （如果已安装预置模块）
- 工作流程管理 （如果已安装预置模块），包括重指派或终止正在进行的工作流程的功能
- 基于 Eclipse 的设计程序，用于创建自定义目录提取定义和关系

更全面的功能列表请参见下表。

功能	说明
基于标准的、浏览器诊断的、可扩展的万维网 UI 用户环境	管理员可更改页布局、默认 （主）页、添加新页和修改全局外观 （主题）。
	通过添加遵从 JSR 168 的入口小程序可扩展用户应用程序。
供应工作流程 （已安装预置模块）	管理员可创建定制的工作流程来处理供应请求。
	这些工作流程又可由拥有适当权限的终端用户启动。
事件驱动的工作流程 （已安装预置模块）	除了用户启动的工作流程，管理员还可以这样配置工作流程：当 Identity Vault 中出现指定的事件时，工作流程会自动激发。
增强型白页	按字母顺序、地理位置、技能集等显示用户信息。
组织结构图	此用户应用程序包含高级组织图入口小程序，它可通过 AJAX 向您提供丰富的交互体验。

功能	说明
用户搜索	用户可执行身份搜索，并保存自定义搜索定义供以后重复使用。
口令自助服务	此用户应用程序允许终端用户访问口令管理功能，从而可减少服务台呼叫数。
轻量级用户管理	用户应用程序允许非 IT 管理员的终端用户执行有限的一组身份管理杂务。
基于 Eclipse 的设计程序	使用设计程序应用程序，系统管理员、开发者、顾问和其他 IT 专家可以快速、轻松地执行各种配置和其它任务。例如，设计程序允许用户脱机使用实体定义和关系、驱动程序策略和过滤器、以及各种驱动程序和驱动程序集配置任务。更改可保存在项目中和 / 或上载到 Identity Vault 中。
代理职能 （已安装预置模块）	用户应用程序用户界面允许拥有适当权限的个人为特定用户定义代理职能。 （代理可代表其他用户执行任务，并拥有该用户的所有权限。）
任务委托 （已安装预置模块）	用户界面允许经理 （以及拥有适当权限的用户）在某个用户的不可用的情况下为同级设置自动任务委托。委托的精密之处在于，特定类型的任务可以委托给不同的个人。
目录提取层	运行时框架将万维网应用程序逻辑与低级别的 Identity Vault 访问和工作流程机制隔离，以获得一个安全、可靠的目录提取体系结构。这种隔离可通过一个叫做目录提取层 （简称提取层）的调解层实现。
对所有面向用户的数据进行访问控制	提取层使用 eDirectory 复杂的有效权限模型，可自动限制身份数据、工作流程以及用户数据修改权限的可见性，其方式对用户甚至入口小程序本身都是透明的。
终端用户身份数据校验	此用户应用程序可向用户提供查看和验证 / 更新各自身份信息的方法， Identity Vault 中描述了这些信息。
灵活的日志记录	可轻松将多种事件记录到服务器日志 （通过 log4j）和 / 或 Novell Audit 中。
Novell Audit Reports	此产品包含预先设定模板的 Crystal Reports，这些报告反映出与供应相关的常用报告任务。
高可用性	可以将此用户应用程序和产品的批准流程要素组成群集，以提高可伸缩性。 重要 **:** 在此版本的预置模块中，不支持对进行中的工作流程实例进行自动故障切换。但是，如果某进行中的流程已中断，则可通过手动干预步骤在剩余的服务器节点上完成该流程。
电子邮件模板管理 UI	使用 iManager 关联和自定义工作流程的电子邮件模板。
附属入口小程序	此用户应用程序附带了多种现成的入口小程序，包括 GroupWise、Exchange、Lotus Notes、万维网邮件、网络文件、 NetStorage、 HTML、快捷方式、 RSS 的入口小程序和讯息入口小程序。

这些功能是 Identity Manager 提供的标准功能外的附加功能。有关产品标准功能集的更多信息，请参见 《*Identity Manager* 管理员指南》。

1.1 支持的职能类型

Identity Manager 用户应用程序包含许多身份管理功能。并非每个用户都需要使用 （也不都能看到）每种类型的功能；功能取决于用户的职能。

假设用户分成以下一个或多个类别，每个类别都有不同的工具和功能。 （本文档中将使用以下词汇表。）

1.1.1 LDAP 管理员

LDAP 管理员是对 Identity Vault （eDirectory 8.7.x 或 8.8）具有最高配置和系统管理权限的人员。这是一个逻辑职能，也可由用户应用程序管理员 （参见下文）共享，该管理员是对应用程序服务器 (JBoss)、数据库 （例如 MySQL）和 / 或基于入口小程序的万维网 UI 自身拥有系统权限的个人或实体。

LDAP 管理员可从以下两种类型的工具中进行选择以完成此工作：用于 Identity Manager 偶然任务 （可能一次）的基于 Eclipse 的设计程序，以及用于日常管理任务的 iManager 工具。

通常在 Designer for Identity Manager 中执行的偶然任务包括：

- 配置可在 Identity Manager 用户应用程序中使用的提取层定义、特性和关系。 （有关更多信息，请参见第 4 章 “配置目录提取层”在第 69 页章节。）
- 验证目录提取层定义。 （请参见第 4 章 “配置目录提取层”在第 69 页章节。）
- 更改用户应用程序驱动程序设置。 （请参见第 3 章 “配置用户应用程序驱动程序”在第 49 页章节。）
- 本地化实体和特性显示标签的显示文本；组织图关系名称；以及全局和本地列表项目。（请参见第 4 章 “配置目录提取层”在第 69 页章节。）
- 导入或导出用户应用程序驱动程序及其设置。
- 其它类型的脱机任务。

在 iManager 中完成管理员 （不管是 LDAP 管理员还是用户应用程序管理员，描述如下）通常在当前系统上执行的日常任务。这些任务可能包括：

- 管理电子邮件模板。
- 定义或指定受供资源和供应请求定义。
- 启用或禁用工作流程定义，从而使它处于活动或不活动状态。
- 终止进行中的工作流程。
- 对 Novell Audit 日志记录的数据运行报告。

其中一些任务 （与工作流程相关的任务）只有在安装了预置模块的前提下才适用。另外，某些任务可能由用户应用程序管理员 （参见下文）而不是 LDAP 管理员执行。

1.1.2 用户应用程序管理员

用户应用程序管理员执行与管理万维网应用程序 （在 JBoss 上运行的基于浏览的应用程序）关联的任务。可通过 Identity Manager 用户界面的 《管理》选项卡访问此职能的管理工具。

可能在用户应用程序中实施的操作包括：

- 配置各种应用程序设置，例如告知用户应用程序如何连接到 Identity Vault （LDAP 提供程序）的设置。有关详情，请参见第 10 章 "入口配置" 在第 183 页。
- 确定 Identity Manager 用户界面中显示的页以及有权访问它们的用户。（请参见第 7 章 "页管理" 在第 125 页。）
- 确定 Identity Manager 用户界面中可用的入口小程序以及有权访问它们的用户。（请参见第 9 章 "入口小程序管理" 在第 165 页。）
- 确定 Identity Manager 用户界面的外观。（请参见第 8 章 "主题配置" 在第 159 页。）
- 控制您希望 Identity Manager 用户应用程序生成的日志记录讯息的级别以及哪些讯息（如果有）将发送到 Novell Audit 中。（请参见第 12 章 "日志记录配置" 在第 193 页。）
- 管理 Identity Manager 用户应用程序维护的各种超速缓存。（请参见第 13 章 "超速缓存配置" 在第 199 页。）
- 导出或导入 Identity Manager 用户应用程序中使用的万维网内容 （页和入口小程序）。（请参见第 14 章 "用于导出和导入入口数据的工具" 在第 207 页。）
- 为特定的个人设置代理权限。
- 很多与用户界面相关的、终端用户可以看到的其它任务。

可以在 iManager 中执行的任务包括：

- 管理电子邮件模板。
- 定义或指定受供资源和供应请求定义。
- 启用或禁用工作流程定义，从而使它处于活动或不活动状态。
- 终止进行中的工作流程。
- 对 Novell Audit 日志记录的数据运行报告。

其中一些任务 （与工作流程相关的任务）只有在安装了预置模块的前提下才适用。

1.1.3 终端用户

终端用户是指能查看共同组成了用户应用程序用户界面的各种入口小程序和万维网页并与之交互的用户。在此环境中，终端用户可以是员工、经理，也可以是员工或经理的代理或受托人。

终端用户可拥有众多潜在的功能，这取决于管理员启用了多少功能。终端用户至少可使用 Identity Manager 用户应用程序进行以下操作：

- 使用组织结构图入口小程序查看用户对象之间的分级关系。
- 查看和编辑用户信息 （拥有适当的权限）。
- 使用高级搜索准则搜索用户或资源 （可保存供以后重复使用）。
- 取回忘记的口令。
- 给小组成员发送电子邮件 （个人或全体）。

另外，如果已安装预置模块，用户应用程序的万维网界面允许用户：

- 请求资源 （启动多个潜在的预定义工作流程之一）。
- 查看以前请求的状态。

- 声明任务和查看任务列表 （通过资源、收件人或其它特征）。
- 查看代理指派。
- 查看委托指派。
- 指定某人的 （不）可用性。
- 进入代理方式以代表他人获得任务。
- 查看小组任务、请求小组资源等 （仅限管理员）。



1.1.4 委托用户

委托用户 （受托人）是一个终端用户，可以向他委托一个或多个特定的任务 （适合该用户权限的任务），这样受托人可替代他人处理这些特定的任务。例如，约翰准备休假，他想让玛丽在他离开的时候处理他的任务。假设玛丽对约翰委托的某一 （或某些）任务拥有适当的权限，玛丽就可以成为约翰的受托人。当约翰在此用户应用程序中将自己标记为不可用时，通常出现在约翰的任务列表中的任务就会显示在玛丽的任务列表中。此时，玛丽的职能就是委托用户。她可以将约翰的任务完全声明为自己的任务 （已经不再是约翰的任务）。请将此与下文中的代理用户定义进行对比。

请注意，委托是逐任务进行的。不一定是全是或全非的职责转移 （但在现实中，如果需要，用户界面的确允许将某个用户的所有任务全部委托给某个特定的受托人）。给定的用户可指定多个受托人。每个受托人只负责指定给他或她的任务。 （例如，约翰可能希望让玛丽处理以后的索要名片的任务，而让比尔处理新的 Siebel 帐户请求。）当某一特定类型任务的原始拥有者声明自己不可用时，会自动发生职责转移，即重指派新任务。 （声明者可选择指定每个任务的委托失效期。）为遵守相关规定，将记录职责转移。

有关委托用户的用户界面功能的详细说明，请参见 《*Identity Manager* 用户应用程序：用户指南》的第 1 章。另请参见本指南中的 “供应安全性”在第 291 页 。

1.1.5 代理用户

代理用户是一个终端用户，他通过临时假借另一用户的身份来履行该用户的职能。代理拥有原用户的所有权限。代理之前属于原用户的工作仍属于原用户。例如，约翰要去中国旅游，

他想让他的行政助手克莱夫访问和处理他所有的任务。如果约翰有适当的权限，他可以指定克莱夫为他的代理。（如果他没有适当的权限，用户应用程序管理员可进行此设置。）代理关系建立后，克莱夫可具有两种职能：克莱夫或约翰的职能。行使约翰的职责时，他可以做任何约翰可以做的事。克莱夫完成工作项目时，就好像是约翰自己完成了任务。

请注意，与上一部分描述的委托机制不同的是，代理关系可以让代理用户完全看到（并且有权处理）原用户的任务和设置。另外，在代理行使职能期间，约翰可以访问的任何特性、关系或系统设置都可以由他的代理访问。

委托和代理的另一个区别是，用户可能会将某些任务委托给一个受托人，而将另一类别的任务委托给其他受托人，而代理总是要接管原用户的所有任务。换句话说，如果您指定某人充当您的代理，则可以确信，该代理可以看到并处理您所有的任务，就好像他变成了您一样。

请注意，替代其他用户执行的代理操作也同样在 Novell Audit 中记录为代理操作（以示符合规定）。

有关代理方案的附加信息，请参见 " 配置供应设置 "，该章节出自《*Identity Manager* 用户应用程序：用户指南》。

1.2 数据提取：灵活管理身份的关键

了解 Identity Manager 用户应用程序的关键概念是数据提取，它指的是能够定义、查看和处理目录提取层定义实例。

传统的储存技术（不论是关系数据库、 X.500 目录还是其它储存库）通常要求数据项（数据库中的行、 X.500 目录中的对象等）严格符合定义良好的纲要。对储存数据的查询在复杂性方面不受限制（理论上），数据可包含索引和 / 或回指链接，但实际的数据项本身必须符合固定的定义。另外，前提是适用的纲要不会随时间发生明显的变化。

如果要将信息（可能有完全不同的数据来源，取决于不同的纲要）聚在一起来创建符合任意新（并且可能是临时）纲要的复合数据对象，这可能是个问题。身份数据是个经典示例，因为身份是合成且非静态的。另外，构成某个身份的数据块也可来自不同的来源，每个来源都理所应当由管理员来适时地保护信息。

身份数据的分布式特征给身份管理造成了一些困难，在严格（且受政治限制）的纲要定义中很难解决这一问题。解决此问题的一个方法是将所有身份数据都聚到逻辑库（已实施为目录）中，并根据将传统 LDAP 对象和特性等映射到任意提取层定义和特性的一个或多个逻辑纲要，按需要组合源数据中的逻辑身份。这样一来，身份数据就变得高度合成和动态。更改身份定义并不要求更改 LDAP 纲要。可随意重定义身份对象，以适合特定的应用程序或特定应用程序的特定用户。

这一总体方法通常称为数据提取，意思是按照需要将身份具体化为所需的格式。

身份数据提取具有很多优点：

- 可避免对 LDAP 目录纲要进行混乱和可产生潜在风险的更改
- 提取技术是非侵入性的，无需更改已连接系统
- 数据之间可以建立新关系
- 可随时更改或扩展提取层定义
- 对象可根据需要拥有任意数量的特性。
- 无关的 LDAP 对象类的特性可合并在提取层定义中
- 命名特性时可使用任意名称（无需使用 LDAP 名称）

- 精密型的访问控制策略仍继续适用 （用户只能查看他们有权看到的数据）
- 可对新对象类型 （或特性组合）执行复杂的搜索，这在纯 LDAP 环境中是不可能做到的

Identity Manager 通过提取实现所有上述目的和更多目的。

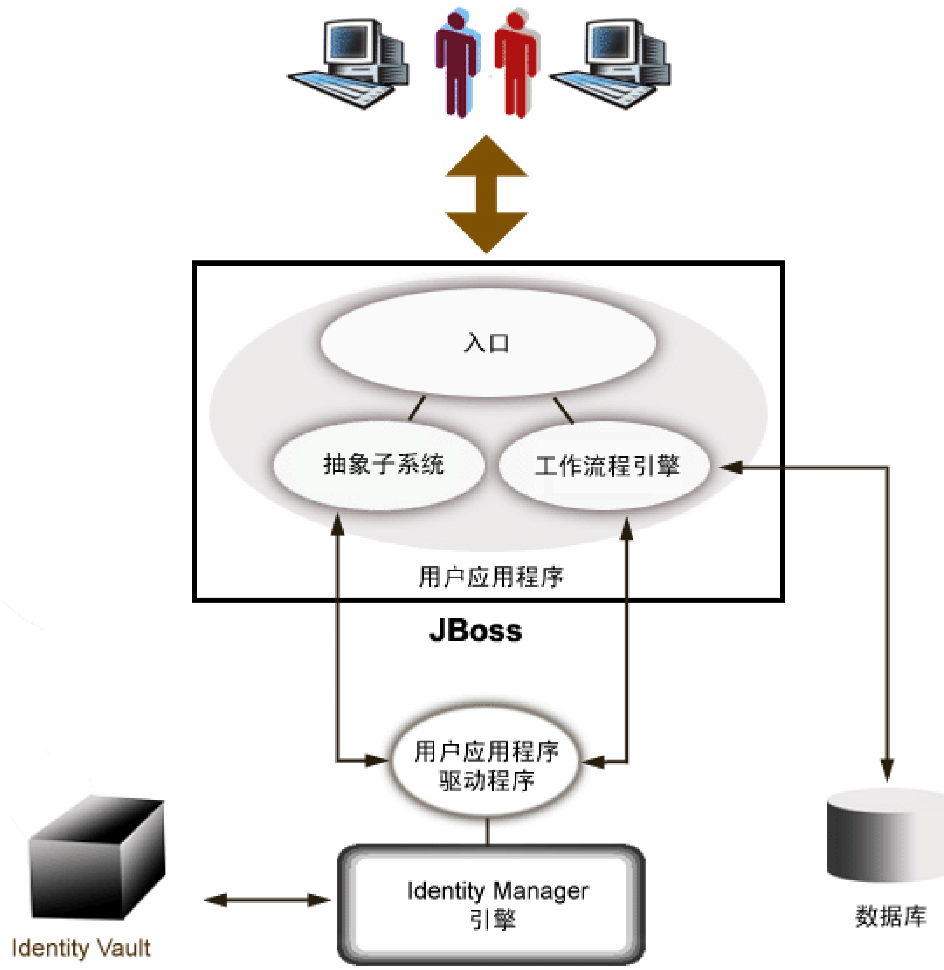
1.3 高级体系结构概述

Identity Manager 用户应用程序依靠一起工作的多个独立部件运行。下表中描述了其中的核心部件及其基本职责。

部件	说明
Identity Vault（eDirectory 8.7.3 或 8.8）	用户数据 （以及其它身份数据）、 IDM 驱动程序集和驱动程序，以及各种提取层物件和工作流程物件 （如果已安装预置模块）的储存库。
Identity Manager 引擎	它是 Identity Manager 运行时框架，用于监视 eDirectory （和已连接系统）中的事件，实施策略、以及在自身和 Identity Vault 间传送数据。
用户应用程序驱动程序	用户应用程序驱动程序与用户应用程序进行通讯，并可在提取层定义被更改时，使后者刷新它的超速缓存。如果安装了预置模块，则还可以将用户应用程序驱动程序配置为允许 Identity Vault 中的事件触发工作流程。它还将权利信息传送回 Identity Vault，这样当工作流程完成时，可以记录是否授予了权利。
用户应用程序：万维网 UI	用户应用程序的万维网 UI 是一个基于浏览器的 Java 应用程序，其中插入了遵从 JSR 168 的入口小程序。
用户应用程序：提取层	提取层将演示层逻辑与 Identity Vault 隔离，以便身份数据的所有请求都必须经过提取层。入口小程序代码无法直接访问身份信息。所有的请求都要经过提取层，并受其控制 （例如，访问控制）。
用户应用程序：工作流程引擎 （仅可用于预置模块）	工作流程引擎是一组 Java 可执行文件，它们负责管理和执行管理员定义的工作流程中的步骤。
JBoss 应用程序服务器	开放源代码 JBoss 应用程序服务器提供运行时框架，在其中可以运行用户应用程序、提取层和工作流程引擎。
数据库 （默认情况下为 MySQL）	数据库 （有关受支持的数据库列表，请参见安装指南）代表用户应用程序储存某些类型的配置信息，以及工作流程状态 （如果已安装预置模块）。
编辑器服务驱动程序	编辑器服务驱动程序是用户应用程序驱动程序的一部分，可将其自定义配置为通过触发工作流程来响应 Identity Vault 事件。
Novell Audit	Novell Audit 是一个独立的日志记录服务器，可保存多种类型的数据（如由工作流程步骤生成的数据）。有关更多信息，请参见本书下文中关于设置日志记录的章节。

从信息流来看，上面提到的部件在逻辑上都以下图描述的方式进行链接。从物理上看，各个部件可能 （大多数情况下会）位于多台计算机上。例如，尽管 Identity Vault （及其主管理工具 iManager）将共同位于承载 Identity Manager 引擎的计算机上，但 JBoss （和用户应用

程序）通常却会驻留在单独的计算机上 （如果已组成群集，则位于一组计算机上）。同样，出于性能、安全和灾难恢复的原因，数据库 (MySQL) 通常位于自己的计算机上。



1.3.1 Identity Vault

Identity Vault 用于储存身份数据和各种类型的提取层定义。eDirectory 的一个实例 （在 Windows、 Solaris 或 Linux 上运行）就用于此目的。通过使用 eDirectory， Identity Manager 能够利用经过充分验证的、伸缩性极强的企业级 LDAPv3 目录 （带分区和复制功能），以及灵活的基于万维网的管理和配置工具 (iManager)，该工具提供了 Identity Manager 和 eDirectory 之间的一体化管理集成点。

1.3.2 JBoss

用户应用程序包装为 Java 万维网应用程序存档 （即 WAR 文件）。WAR 被部署到 JBoss 中，JBoss 是一种常见的开放源代码 Java 应用程序服务器 （使用 Tomcat 作为服务器小程序引擎 ；未显示在图中）。将 JBoss 用作执行环境有很多优点，包括：

- 可免费获得源代码。
- 从 4.0.3 版开始，可将 JBoss 组成群集。

- JBoss 完全符合 J2EE，这意味着任何 J2EE 应用程序都可以在它上面运行。您可以在用户应用程序运行所在的 JBoss 的同一实例上承载其它应用程序（例如， Web Services）。
- JBoss 支持标准 JAAS 和 JACC Java 安全和授权服务 （用户应用程序依靠它来访问 Identity Vault）。
- JBoss 可在多个不同的平台上运行，包括 Windows 和 Linux 的常用版本。

用户应用程序 WAR 包含用户应用程序的可执行代码。出于隔离目的，可执行代码又使用模型视图控制器 (MVC) 体系结构来构建。面向用户的界面在用户应用程序中作为模块化入口小程序运行。单独的入口小程序用来查看组织结构图、进行搜索、查看用户细节、重设置口令等。

有关向 JBoss 部署万维网应用程序的各个方面的更多信息，请参考 JBoss 文档，网址为 http://www.jboss.org/products/jbossas/docs (http://www.jboss.org/products/jbossas/docs)。

1.3.3 数据库

用户应用程序依靠数据库 （默认情况下为 MySQL ；有关受支持的数据库列表，请参见安装指南）来储存多种类型的信息：

- 用户应用程序配置数据：例如，万维网页定义、入口小程序实例注册和自选设置值。
- 如果已安装预置模块，则数据库中会保留工作流程状态信息。 （实际的工作流程定义储存在 Identity Vault 中。）
- Novell Audit 日志

1.3.4 Identity Manager 引擎

Identity Manager 产品包括运行时引擎、驱动程序和策略。Identity Manager 引擎响应 Identity Vault 中的事件，并管理数据在它自身和 Identity Vault 之间的流动和转换。驱动程序对象封装可执行代码和物件 （如策略文档），旨在提供特定于某一已连接系统的数据处理行为。Identity Manager 用户应用程序是一个已连接系统。Identity Vault、用户应用程序的提取层和工作流程引擎之间的通讯通过用户应用程序驱动程序来实现 （参见下文）。

由于用户应用程序依靠多种目录对象来储存提取层物件，因此必须扩展 eDirectory 纲要以容纳用户应用程序所需的自定义 LDAP 对象和特性。在 Identity Manager 安装过程中，会自动进行纲要扩展。但是，只有安装并激活了用户应用程序驱动程序，才会用默认值填充自定义对象和特性。

1.3.5 用户应用程序驱动程序

用户应用程序驱动程序是一个重要的用户应用程序启动块。用户应用程序驱动程序的一个职责就是：在 Identity Vault 中有重要的数据值发生更改时通知提取层，以便提取层更新其超速缓存。

如果已安装预置模块，则可以将用户应用程序驱动程序配置为自动开启工作流程，来响应 Identity Vault 中的特性值更改。

用户应用程序驱动程序不仅是一个运行时部件，也是一个目录对象的储存包装程序 （组成用户应用程序运行时物件）。下面显示与用户应用程序驱动程序相关联的目录物件的典型表示形式。



注释 **:** 显示的名称表示 LDAP 常用名 (cn) 值。各种对象类的实际纲要命名将在别处讨论。

下文更详细地讨论了这些物件类别。

驱动程序集对象

每次安装 Identity Manager 时都需要将驱动程序分组为多个驱动程序集。在给定的目录服务器上，每次只能有一个驱动程序集处于活动状态。可以单独打开或关闭集内的驱动程序，而不会影响作为整体的驱动程序集。与其它任何 IDM 驱动程序类似，用户应用程序驱动程序必须存在于驱动程序集的内部。用户应用程序不会自动创建驱动程序集；必须事先创建一个驱动程序集，然后在其内部创建用户应用程序驱动程序。

用户应用程序驱动程序

用户应用程序驱动程序对象 （可赋予任意名称）是多种物件的树枝。像所有 Identity Manager 驱动程序一样，用户应用程序驱动程序执行发布者和订购者通道对象和策略。虽然发布者通道可用于自定义使用的情况，但不可用于用户应用程序。

应用程序配置对象

AppConfig 对象是各种用户应用程序配置对象的树枝：

RequestDef

它是供应请求定义的树枝，供应请求定义是管理员配置的请求定义，可用于用户应用程序运行时 （如果存在预置模块）。这种树枝中存储的定义 （作为 XML 存储）表示具有相应权限

的终端用户可通过用户应用程序实例化的请求的类。RequestDef 将 WorkFlowDef （见下文）与 ResourceDef 相关联。

WorkFlowDef

工作流程对象的树枝，包括设计时说明和所有模板或未使用的流程。

ResourceDef

受供资源定义的树枝，包括设计时说明和所有模板或未使用的目标。

ServiceDef

服务定义对象的树枝，用于包装工作流程调用的 Web Services。

DirectoryModel

提取层元级别的对象 （ChoiceDef、 EntityDef、 RelationshipDef），表示可由身份入口小程序公开的目录的不同类型的内容 （部分可由用户定义，其它由管理员设置）。

AppDef

用于初始化运行时环境 （例如，超速缓存配置信息和电子邮件通知属性）的配置对象的树枝。

ProxyDef

代理定义的树枝。

DelegateeDef

委托定义的树枝。

1.3.6 目录提取层

入口小程序通过查询目录提取层来获取它们的身份数据，目录提取层是将身份数据访问的细节与客户程序进程相分离的代码层。例如，当入口小程序需要搜索身份数据时，提取层将代表入口小程序对 Identity Vault 中的目标树枝进行适当的 LDAP 查询。所有入口小程序在任何时候都不会直接查询 Identity Vault。

目录提取层还是创建和更改提取层定义的代码层，这些定义由系统管理员或其他有资格的用户指定。若要进行此类更改，系统专家将使用设计程序应用程序的目录提取层编辑器，有关此编辑器的说明，请参见本指南中的第 4 章 “配置目录提取层”在第 69 页 。

在运行时，提取层将超速缓存 Identity Vault 中包含的多种配置和实体定义数据。用户应用程序维护的各种超速缓存可由管理员细化管理。有关超速缓存和超速缓存管理的附加信息，请参见第 13 章 “超速缓存配置”在第 199 页 。

1.3.7 工作流程引擎

工作流程引擎 （安装预置模块时可用）是一组运行时类，负责执行由进程定义 （实例化工作流程时创建的运行时物件）指定的工作流程步骤，并跟踪数据库 （如 MySQL 或 Oracle ）中保存的状态信息；请参见上文中的 “数据库”在第 21 页 。

有关工作流程系统的附加详情，包括如何创建工作流程，请参见本指南下文中的第 21 章 “基于工作流程的配置信息提供的介绍”在第 283 页 。

1.3.8 用户界面

Identity Manager 用户界面由与 JSR168 兼容的入口小程序集合 （在安装预置模块后，还包括一些 Java 服务器页）组成，它们运行在基于 JBoss 的 Java 万维网应用程序中。入口小程序体系结构可提供较高的模块化程度，内容的自定义以及实现用户对页面外观的控制。用户应用程序框架可提供多种类型的树枝服务。它管理窗口状态、入口小程序自选设置、持久性、超速缓存、主题设置和日志记录等，并担当安全性门卫。运行该用户应用程序的应用程序服务器又可向该应用程序提供多种服务，例如通过群集实现可伸缩性、通过 JDBC 访问数据库以及支持基于证书的安全性等。

此体系结构具有高度的封装性，为 Identity Manager 用户应用程序提供强大、安全的演示层环境。它也保证对用户界面所有方面的高度管理控制。

有关对用户界面各部分进行管理的更多信息，请参考本指南“管理用户应用程序”在第 117 页 中的各章节。

1.4 设计和配置工具

通过 Identity Manager 设计程序工具 （基于 Eclipse Rich Client Platform）或 iManager 插件，可以对多种 Identity Manager 用户应用程序功能进行自定义或自定义配置。

下表说明了可用的工具及其用途。

工具	用途
Designer for Identity Manager	Identity Manager 的常规配置工具，允许开发者、顾问或系统管理员对驱动程序集、驱动程序、策略定义和其它物件进行详细的配置更改。
设计程序的目录提取层编辑器插件	允许定义自定义对象和关系，以及对提取层的各种配置设置进行更改。请参见本指南下文中的第 4 章 “配置目录提取层”在第 69 页 。
供应请求配置插件	允许定义和配置可用的供应请求类型 （iManager 中）
受供资源编辑器 （即将推出）	允许创建和配置资源的设计程序插件 （表示将根据工作流程授予的资源的对象）
工作流程定义编辑器 （即将推出）	设计程序的图形工作流程定义插件
工作流程电子邮件模板编辑器	允许管理员添加、删除和编辑电子邮件模板的 iManager 插件。工作流程系统可使用这些模板向用户通知工作流程事件。
lreport.exe （日志报告工具）和 iManager 审计和日志记录功能	（Identity Manager 附带的）许多预定义的日志报告都提供 Crystal Reports (.rpt) 格式，以过滤记录到 Novell Audit 数据库中的数据。**lreport.exe** 日志报告工具 （仅限 Windows）是生成报告的一种方式。也可以使用其它方法创建报告；有关详情，请参见第 5 章 “设置日志记录”在第 109 页 。

系统设计专家通常先使用目录提取层编辑器 （在 Designer for Identity Manager 中）设置用户应用程序的自定义提取层定义。这些对象随后可供提取层使用，因而也可供用户界面的用户使用。精确的访问控制设置可用于这些对象的定义和使用中，这样管理员和最终用户就只能查看和操纵自己具有相应权限的对象 （以及这些对象上的特性）。

如果已安装预置模块，则系统设计专家或管理员将使用 iManager 中的 《供应请求配置》向导，定义将供用户应用程序的用户使用的受供资源和工作流程。同时，管理员会使用电子邮件模板编辑器功能 （iManager 中），定义工作流程将发送的电子邮件通知的正文内容。有关此问题的更多信息，请参见第 23 章 “管理供应工作流程”在第 317 页 。

配置提取层、供应请求定义、审计要求和电子邮件模板之后，管理员通常会使用第 10 章 “入口配置”在第 183 页中说明的管理功能，执行影响用户应用程序的各项配置操作 （涉及安全性、超速缓存和其它功能）。最后，管理员会根据需要，使用本指南第 IV 部分中各章节介绍的界面，配置单个入口小程序。

注释 **:** 下一章更详细地说明了其中的一些任务，因此在实施生产环境前应首先参考此章节。

1.5 使用方案

Identity Manager 用户应用程序中提供了大量的功能。下面的几个示例将深入讨论使用用户应用程序解决现实问题的方法。

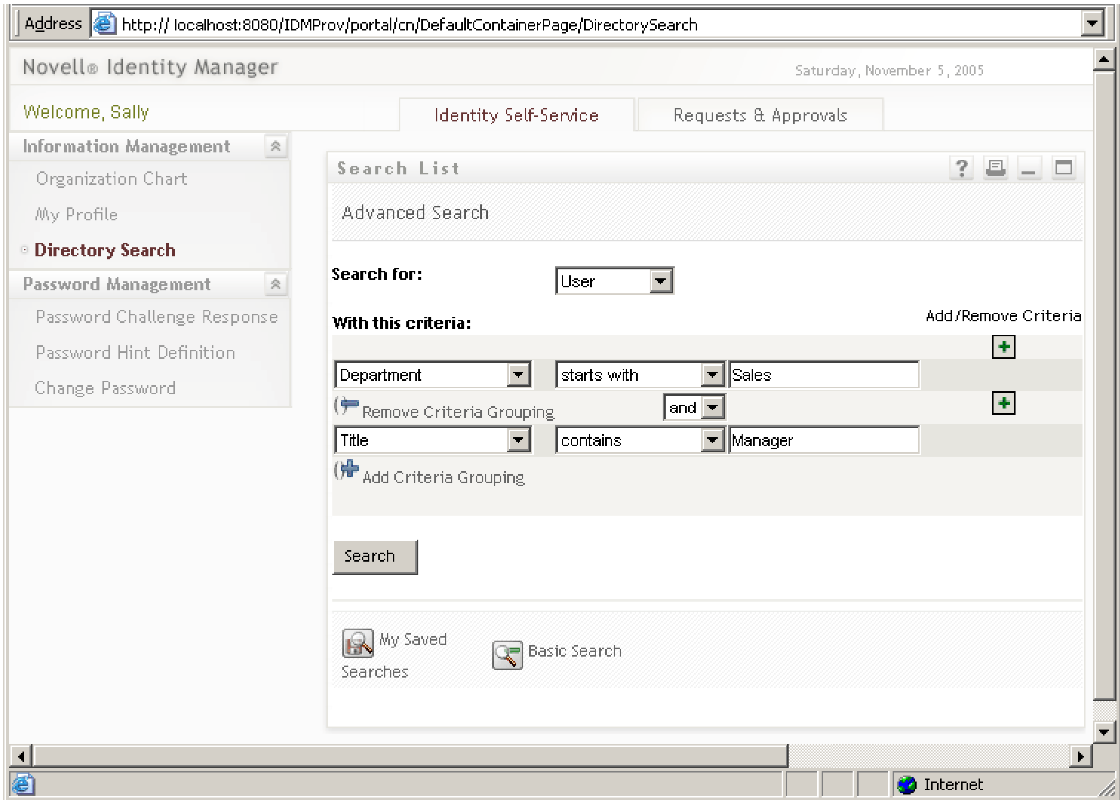
1.5.1 方案 A：用户搜索有关组织中其他人员的信息

常见应用案例是某员工希望找到有关组织中其他人员的信息。例如：

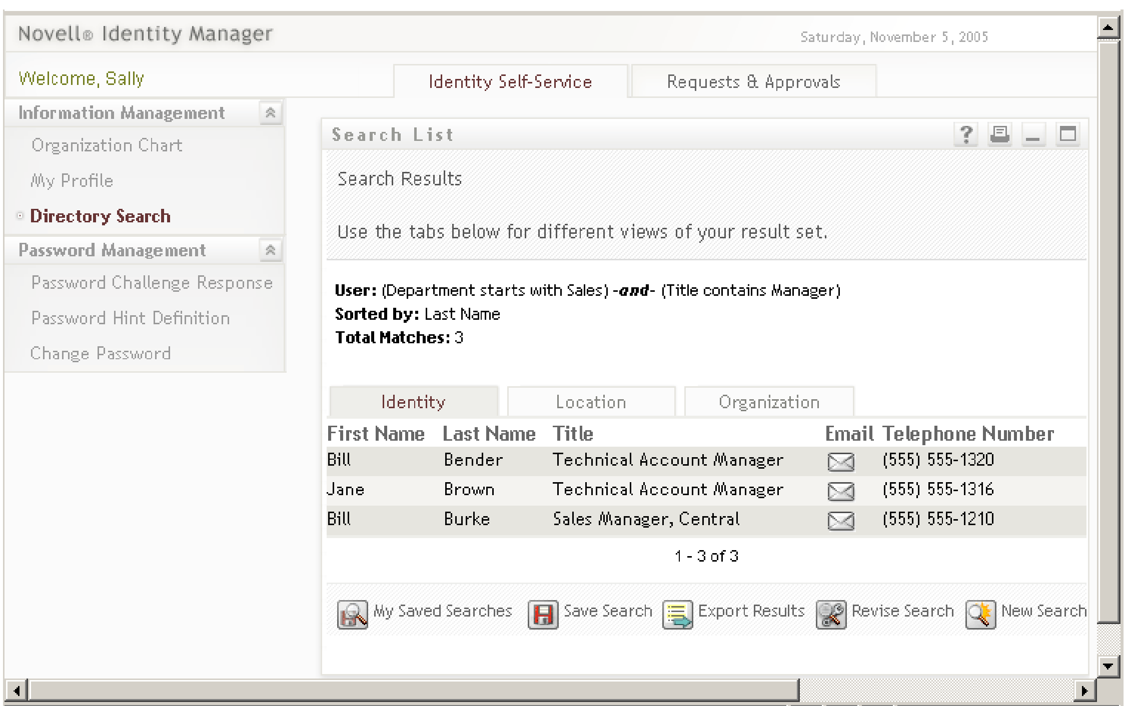
- 获取同事的全名和联系信息
- 查找某个地理范围内具备特定技术的所有人员
- 确定特定人员的经理

通过目录搜索界面可轻松完成这些类型的操作 （包括基于复杂查询的更高级搜索）。通常，终端用户会登录用户应用程序并将 《身份自助服务》选项卡调至前台 （如果它尚未位于顶层），然后单击左侧导航链接列中的 《目录搜索》链接。

在下面的屏幕中，登录用户设置了高级搜索，以查找其部门以 Sales （销售）开头，而 Title （职务）包含 《经理》的用户。



完成此次搜索后，将提供与下图类似的结果屏幕：

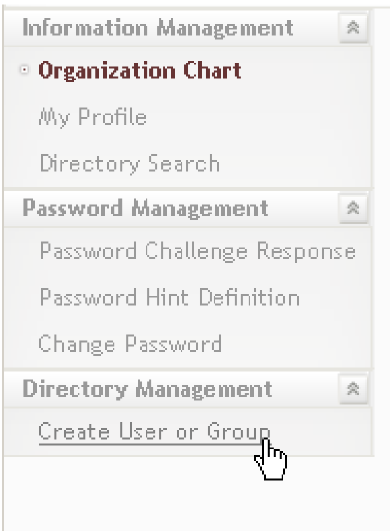


请注意屏幕底部的一排按钮，用户可以使用它们保存特定高级查询、修改查询以及开始新搜索等。另请注意已找到的个人列表上的选项卡。当前个人按 《身份》列出，但也可以使用相应的选项卡按 《位置》或 《组织》进行查看。

1.5.2 方案 B：经理创建新用户

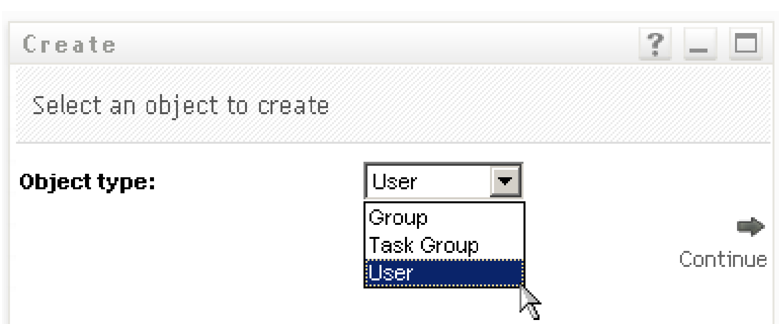
假定公司某部门雇佣了新的实习生、合同工或其他非员工人员 （可能仅为公司工作一段时期）。新进人员需要被输入系统中，以便为其提供相应的有限资源集 （并且可通过上述类型的用户搜索找到他们）。由于该人员不是正式员工，所以不能成为公司常规人力资源系统的一部分。但该人员的身份 （和资源访问权限）仍需得到安全的管理。

作为相关部门的经理，您拥有将用户输入系统的权限。要进行此操作，请登录，并在页左侧的导航链接列中找到 《创建用户或组》链接 （见下图）：

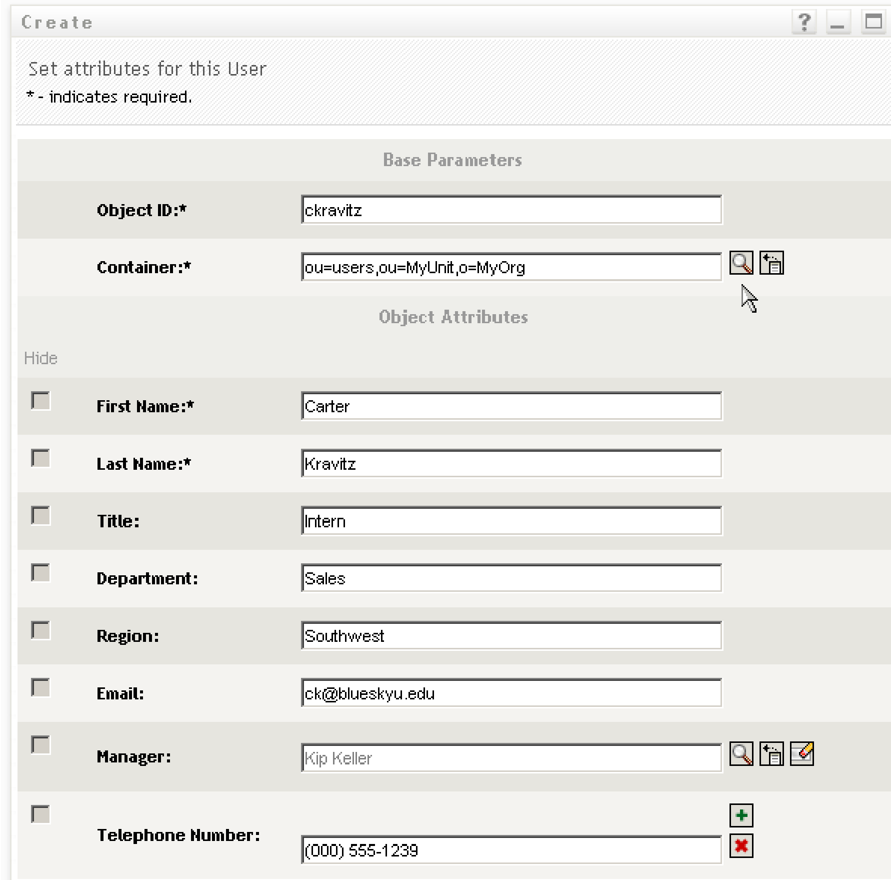


注释：如果登录的用户不具备相应的权限，则不会显示此链接。

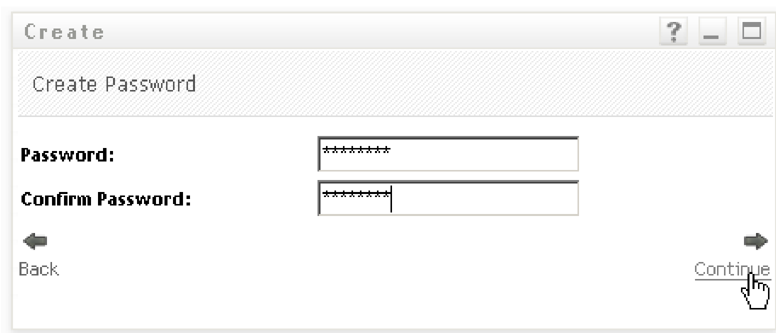
单击此链接之后，将出现一个屏幕，询问希望新建 《组》、《任务组》还是 《用户》（如下图所示）。



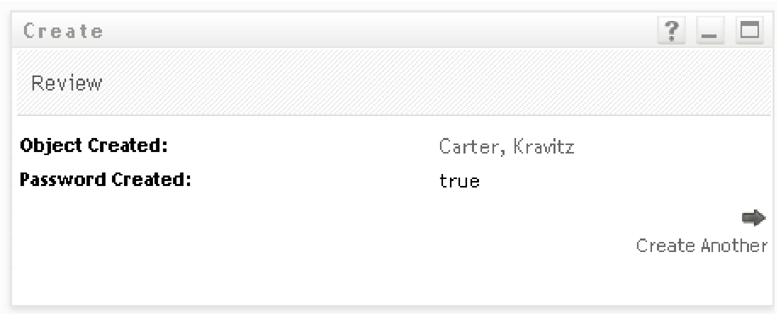
选择 《用户》并单击 《继续》之后，将出现下一个向导面板，您可以在其中输入此用户的个人信息：



下一个屏幕允许您为新用户指派口令：



结束屏幕显示这一过程的最终结果。



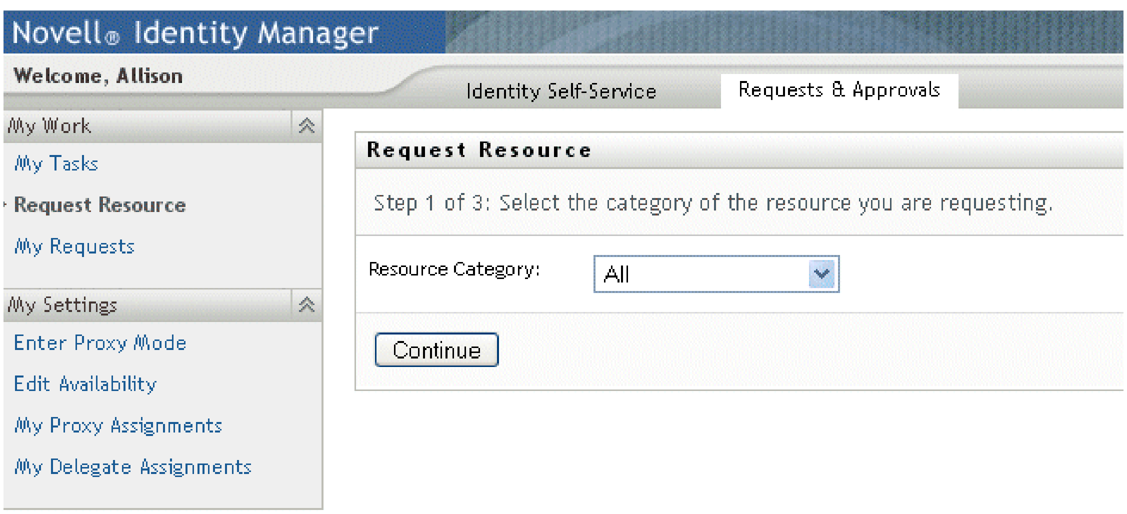
在此示例中，新输入的人员将具备常规用户的所有权限。但可以使用目录提取层编辑器定义 Intern 对象等，使之具有对应于该类对象的唯一特性和权限。在这种情况下， Intern （实习生）将作为一个选项与 《组》、《任务组》和 《用户》一起显示在前面的选择列表中。

1.5.3 方案 C：用户供应

一种常见的情况是，员工在获取资源 （无论是一件办公设备、公司信用卡，还是数据库的访问权）时需要经过其他人员的批准。这种情况称为供应请求。在 Identity Manager 中，如果安装并配置了预置模块，则可以通过工作流程来处理此类请求。

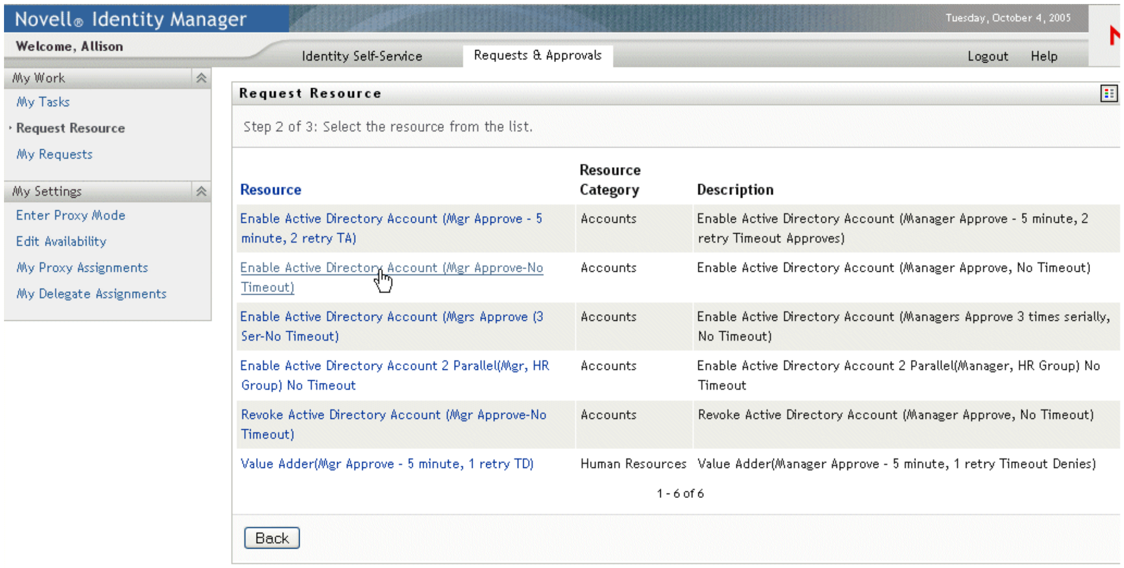
注释 **:** 与之前的示例不同，此示例需要安装和配置预置模块。

用户需要首先登录用户应用程序以进入登录页。在该页的顶部，用户单击 《请求和批准》选项卡，然后找到左侧导航框架中的 《请求资源》链接。单击 《请求资源》链接后，用户应用程序将显示初始请求表格。



《资源类别》下拉菜单可能包含任意多个资源类型，其中包括任意名称的权利 （有关权利以及如何创建权利的更多信息，请参见 Identity Manager 主管理指南）。要查看所有可用的受供资源 （即此特定用户使用其现有权限可请求的所有资源），只需选择 《所有》，如上所示。

如果用户单击 《继续》，则出现下一个屏幕，其中将显示允许此用户访问的所有供应请求类型。



在此示例中，用户希望请求 Active Directory 帐户，这需要经理批准。只需通过单击相应的链接并填写简单的表格，即可启动关联的工作流程，同时此人员的经理将收到一封电子邮件通知，其中包括经理需执行的任务。经理现在可以登录自己的 《请求和批准》页，在任务列表中查找等待批准或拒绝的员工请求。 （如果经理正在休假，则通知他或她指定的代理，该代理可以登录系统并代替经理执行操作。）同时，浏览器屏幕将更改为显示摘要页，确认工作流程请求已成功提交。

授予公司目录中的帐户 （如图所示）是权利请求的一个示例。在 Identity Manager 用户应用程序中，可以配置多种权利请求 , 并且可以创建多种工作流程 （一名或多名经理批准、顺序流程或并行流程、超时或不超时等）。在所有情况下，均可以使用精确的访问控制管理工作流程和其它信息的可见性。

有关这些功能的更多信息，请参见本指南的最后一章。 （这些章节中的信息主要针对管理员。有关这些功能用法的更详细说明，请参见 《Identity Manager 用户应用程序用户指南》。）

1.6 进一步学习

如果准备了解有关设计生产环境的更多信息，请转至下一章 （第 2 章 “设计生产环境”在第 33 页 ）。您也可直接转至本书后面的某一章，获取以下信息：

要了解更多有关用户应用程序的日志记录和审计功能的信息，请参见第 5 章 “设置日志记录”在第 109 页 。

要了解更多有关自定义用户界面的外观与使用体验的信息，请参见第 8 章 “主题配置”在第 159 页 。

要了解更多有关通过用户应用程序管理界面 （而不是 iManager）管理的安全性的信息，请参见第 11 章 “安全性配置”在第 189 页 。

要了解更多有关用户应用程序超速缓存功能的信息，请参见第 13 章 “超速缓存配置”在第 199 页 。

要了解更多有关口令管理功能的信息，请参见第 19 章 “口令管理入口小程序参照”在第 257 页 。

要了解更多有关入口小程序管理的信息，请参见第 9 章 “入口小程序管理”在第 165 页 。

要了解有关导入和导出入口数据的信息，请参见第 14 章 “用于导出和导入入口数据的工具”在第 207 页 。

要了解更多有关组织结构图功能的信息，请参见第 18 章 “组织结构图入口小程序参照”在第 241 页 。

要了解更多有关目录搜索功能的信息，请参见第 20 章 “搜索列表入口小程序参照”在第 269 页 。

要了解更多有关新对象创建 （创建入口小程序）选项及其管理方法的信息，请参见第 16 章 “创建入口小程序参照”在第 221 页 。

要了解更多有关工作流程设置和管理的详细信息，请参考第 21 章 “基于工作流程的配置信息提供的介绍”在第 283 页 、第 22 章 “配置供应请求定义”在第 295 页 和第 23 章 “管理供应工作流程”在第 317 页 。

设计生产环境 2

本章将讨论与设置生产环境相关的问题。在从沙盒 / 测试或其它生产前环境转换至生产环境的过程中，会出现许多需要考虑的事项，本章提供了有关这些事项的指南。

本章的组织主要分以下几个部分：

- “拓朴”在第 33 页
- “安全性”在第 35 页
- “性能调节”在第 37 页
- “群集”在第 40 页

2.1 拓朴

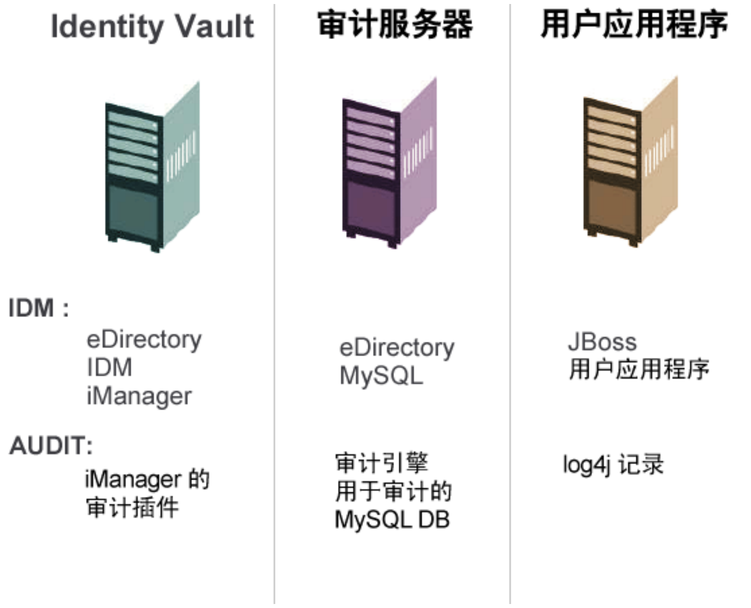
每个主要子系统的实例数量及其连接方式可能为数众多。但并非所有可能的布局都能得到支持。重要的是，除了了解各种可能性之外，还要了解应优先考虑某些配置的原因。

2.1.1 最小设计

此用户应用程序最简单的逻辑配置是一次安装所有项，包扩 Identity Vault 树、 Identity Manager 引擎的实例和驱动程序，以及运行用户应用程序单一实例的 JBoss 实例。在物理实现方面，理论上可以在一台计算机上运行所有的部件。但是由于各种原因 （它们之间的安全性、可维护性以及性能的要求），在实践中可能无法这样做。在决定实际安装中所需的计算机数量时，应该 （至少）考虑以下方面：

- *Novell Audit* 服务器：此组成部分负责在运行时从用户应用程序环境截获事件信息 （可能还有大量的其它信息）。它也可担当另一重任务：公司其它应用程序的永久储存库。由于各种原因，您可能不希望将 Identity Manage 系统的其它主要组成部分 （例如 JBoss 或 Identity Vault）与 Audit 服务器运行在同一台计算机上。
- *Identity Vault*：此部件通讯量巨大，需要良好的性能和可伸缩性。您一定希望 Identity Vault 存在于专用计算机上。换言之，您可能不希望其它高通讯量系统 （例如部署了用户应用程序的 JBoss）与 Identity Vault 在同一台计算机上运行。
- 数据库：如果这个 MySQL （或其它支持的数据库）的实例也是 Novell Audit 数据库，它最好在专用计算机上运行。请考虑由用户应用程序通过以下方式使用此组成部分：
- 作为入口配置数据的永久储存库
- 作为处理中工作流程状态信息的永久储存库 （如果安装了预置模块）
- 另外，还可作为 Novell Audit 的日志记录储存库。
- *JBoss*：由于性能和容量的原因，可能需要在专用计算机上运行此组成部分。

出于以上考虑，建议采用下面最少有 3 台计算机的配置：



2.1.2 高可用性设计

本章后面的部分中详细介绍了用群集来实现高可用性 / 功能。目前，您应该了解：

- Identity Manager 通过多节点安装以及共享储存机制支持 Identity Vault、引擎和驱动程序的高可用性。请参见主 Identity Manager 管理指南中有关 《高可用性》的章节，以获取有关说明。有关使用 SUSE Linux 设置这类系统的综合方案，请访问以下站点中的文章：

  http://support.novell.com/cgi-bin/search/searchtid.cgi?/10093317.htm (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10093317.htm)
- 通过 JBoss 群集，可获得用户应用程序的高可用性。可以设置一个 JBoss 群集，使每个节点运行一个用户应用程序实例。实例之间完全平等 （对等）。但实例间不存在会话复制。每个实例都将负责自己的工作单元，而不会完成在姐妹节点上启动的会话。
- 不支持自动故障转移 （原因同上）。但如果新节点上线时使用宕机节点的同一工作流程引擎 ID，中断的工作流程可以在失去该群集节点后再次恢复。 （在这种情况下，新工作流程引擎一旦启动，中断的工作流程将立即自动恢复。）

有关此问题的更多详细信息，仍请参见下文中的 “群集”在第 40 页 。

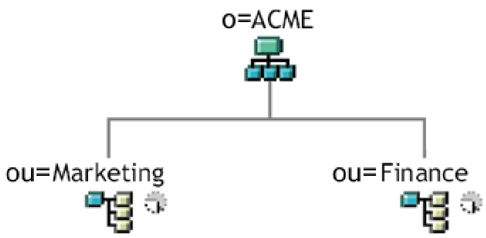
2.1.3 设计限制

总的来说，需要了解的两个最重要的体系结构限制是：

- 一个用户应用程序实例无法为超过一个的用户树枝提供服务 （搜索 / 查询、添加用户等）。此外，一旦用户树枝与应用程序相关联，此关联将是永久性关联。
- 一个用户应用程序驱动程序无法与超过一个的用户应用程序相关联，但在同一 JBoss 群集的姐妹节点上安装用户应用程序的情况除外。换言之，不支持驱动程序到用户应用程序的一对多映射。

第一个限制强化了用户应用程序设计中的高度封装。

假定具有以下组织结构：



安装用户应用程序的过程中，需要指定程序将在 Identity Vault 中查找的顶级用户树枝。在这种情况下，您可以指定 *ou=Marketing,o=ACME* 或 *ou=Finance,o=ACME* （任选其一）。但不能同时指定两者。所有用户应用程序搜索和查询 （和管理员登录）的范围将设定在指定的树枝内。

注释 **:** 理论上，可以指定 *o=ACME* 的范围包括 《Marketing》和 《Finance》。但是在大型组织中，可能有多个 *ou* 树枝 （并非只有与 《Marketing》和 《Finance》相关的两个树枝），因此在实际中这种方法可能行不通。

当然，可以安装两个独立的用户应用程序 （不共享任何资源），一个用于 《Marketing》，另一个用于 《Finance》。每个程序都拥有自己的数据库以及经过适当配置的用户应用程序驱动程序，此外，每个用户应用程序将进行单独管理，并可以具有唯一的主题。

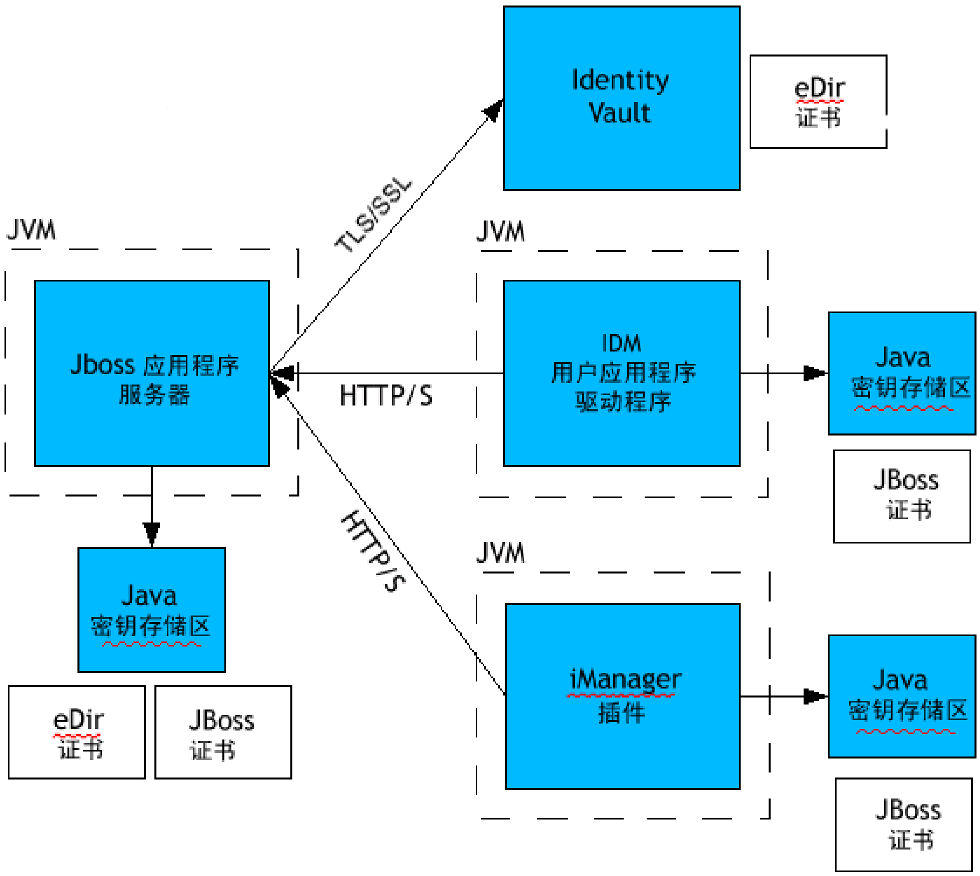
如果确实需要将 《Marketing》和 《Finance》放置在一个用户应用程序的相同范围内，则可以考虑两种方法。一种是在两个姐妹节点之上的层次中插入新树枝对象 （例如 *ou=MarketingAndFinance*）；然后指向新树枝作为范围的根。另一种方法是创建一个组合了原始 ACME 树中所需部分的已过滤复本 （一种特殊的 eDirectory 树），并指向位于复本根树枝处的用户应用程序。 （有关已过滤复本的更多信息，请参考 《Novell eDirectory 管理指南》。）

如果您有关于特定系统布局的问题，请联系 Novell 代表以获取帮助或建议。

2.2 安全性

从生产前阶段过渡到生产阶段通常要强化系统的安全性。在沙盒测试阶段，可能一直使用常规的 HTTP 将用户应用程序驱动程序连接到 JBoss，或使用自我签名证书 （作为临时措施）进行驱动程序 / 应用程序 - 服务器之间的通讯。另一方面，在生产阶段，可能会使用安全连接，采用基于公司的 Verisign （或其他可信提供者）证书的服务器鉴定。

通常情况下， X.509 证书普遍应用于 Identity Manager 用户应用程序环境中，如下图所示。



默认情况下，在用户应用程序和 Identity Vault 之间使用传输层安全性进行的所有通讯都是安全的。安装时会自动将 Identity Vault (eDirectory) 证书安装至 JBoss 密钥存储区。除非另行指定，用户应用程序安装程序会将 eDirectory 证书的副本置于 JRE 的默认 *cacerts* 存储区中。

若要确保通讯安全，服务器证书需放置在多个位置，如图所示。根据您是要在图中显示 *JBoss cert* 框的各个位置使用自我签名证书，还是使用由可信证书授权者 (CA) （例如 Verisign）颁发的证书，所需的设置步骤可能会有所不同。

自我签名证书

如果使用著名的可信颁发者的证书 （例如 Verisign），则无需进行特殊的配置步骤。但如果要创建并使用自我签名证书，则需要执行以下步骤：

1 使用类似以下语法的命令行语法，创建一个具备自我签名证书的密钥存储区：

```
keytool -genkey -alias tomcat -keyalg RSA -storepass changeit -
keystore jboss.jks -dname
"cn=JBoss,ou=exteNd,o=Novell,l=Waltham,s=MA,c=US" -keypass
changeit
```

注意，创建证书的同时，还将创建 《jboss.jks》文件。

2 将密钥存储区文件 (jboss.jks) 复制到 JBoss 用户应用程序目录中，例如：

```
cp jboss.jks ~/jboss-4.0.2/server/spitfire/conf
```

打开 **JBoss** 中的 **SSL**

要在 JBoss 中启用 SSL，请在 *[IDM]/jboss/server/IDM/deploy/* 目录下找到 *jbossweb-tomcat55.sar* 文件。在其中找到 *server.xml*，然后在文本编辑器中打开此文件。通过取消注释或添加如下部分启用 SSL：

```
<Connector port="8443" address="${jboss.bind.address}"
maxThreads="100" strategy="ms" maxHttpHeaderSize="8192"
emptySessionPath="true" scheme="https" secure="true"
clientAuth="false" keystoreFile="${jboss.server.home.dir}/spitfire/
conf/jboss.jks" keystorePass="changeit" sslProtocol = "TLS" />
```

打开 **SOAP** 安全性

在 *IDM.war* 中，找到 *web.xml* 文件，然后在文本编辑器中打开此文件。在文件的底部，去掉以下部分的注释标记：

```
<security-constraint> <web-resource-collection> <web-resource-
name>IDMProv</web-resource-name> <url-pattern>/*</url-pattern> <http-
method>POST</http-method> <http-method>GET</http-method>
<description>IDM Provisioning Edition</description> </web-resource-
collection> <user-data-constraint> <transport-guarantee>CONFIDENTIAL</
transport guarantee> </user-data-constraint> </security-constraint>
```

保存文件和存档。重启动 JBoss。

2.2.1 相互鉴定

Identity Manager 用户应用程序支持传统的服务器鉴定 方案 （在万维网上，通常与安全万维网页 共同用于 https 会话），但不支持框外基于证书的双向鉴定。但是，可以通过使用 Novell iChain 获得该功能。因此，比如说，您的组织需要允许用户通过用户证书而非口令进行登录，则可以通过将 iChain 添加到您的环境中来达到此目的。

有关更多信息，请与您的 Novell 代表联系。

2.3 性能调节

性能调节是一个复杂的话题。Identity Manager 用户应用程序依赖许多技术的大量交互过程。因此，无法预测哪个单独的配置方案或用户交互方案可能导致性能降低。尽管如此，部分子系统仍可采用能够增强性能的最佳做法。以下是对这些做法的说明。

2.3.1 日志记录

用户应用程序允许通过 Novell Audit 和开放源代码的 Apache *log4j* 框架进行日志记录。默认情况下不通过 Novell Audit 记录日志，但将启用通过 *log4j* 进行文件和控制台日志记录。

注释：有关可以记录日志的事件类型，以及如何启用或禁用日志记录，可参见本指南下文中的第 5 章 “设置日志记录” 在第 109 页和第 12 章 “日志记录配置” 在第 193 页。

log4j 配置设置包含在 *$IDMINSTALL/jboss/server/IDMProv/conf/* 下名为 *log4j.xml* 的文件中。在该文件的底部，您将找到以下项：

```
<root>     <priority value="INFO" />     <appender-ref ref="CONSOLE" /
>     <appender-ref ref="FILE" /> </root>
```

为 root 赋值，以确保不具备显式指派级别的任何日志附加程序继承 root 的级别 （在此例中为 INFO 级别）。例如，默认情况下，未对 FILE 附加程序指派阈值级别，所以它采用了根的阈值级别。

根据 *org.apache.log4j.Level* 类中的定义， *log4j* 可能使用的日志级别包括 DEBUG （调试）、 INFO （信息）、 WARN （警告）、 ERROR （错误）和 FATAL （致命）。不注意正确使用这些设置将严重降低系统的性能。

一个好的经验是仅在调试特定问题时才使用 INFO 或 DEBUG 级别。

对于设置了级别阈值的根中的任何附加程序，只要不进行调试操作 （如前所述），都应将其阈值设置为 ERROR、 WARN 或 FATAL。

就高日志级别对性能的影响而言， *log4j* 中控制台和文件日志记录 （涉及同步写入）的影响要大于讯息冗长的影响。可以使用 AsyncAppender 类，但使用它不能保证更佳的性能。有关这些问题 （众所周知的 Apache *log4j* 问题，而非 Identity Manager 问题）的说明，请访问 *http://logging.apache.org/log4j/docs/api-1.2.8/org/apache/log4j/performance/Logging.html*。

用户应用程序日志配置文件 （见上文）中的 INFO 默认级别可满足多种环境，但是在性能至上的场合，则需考虑将上面的 *log4j.xml* 项更改为：

```
<root> <priority value="ERROR"/> <appender-ref ref="FILE"/> </root>
```

也就是说，要去除 CONSOLE 并将日志级别设置为 ERROR。对于经全面测试 / 调试的生产设置，无需以 INFO 级别记录日志，也无需将 CONSOLE 日志记录保留为启用状态。关闭这些设置所带来性能收益会非常显著。

有关 *log4j* 的更多信息，请参考 *http://logging.apache.org/log4j/docs* 中提供的文档。

有关更多与 Identity Manager 一起使用 Novell Audit 的信息，请参考 《Novell Identity Manager 管理指南》。

2.3.2 Identity Vault

LDAP 查询在高占用率目录服务器环境中可能会成为瓶颈。为了保持处理大量对象时的高性能， Novell eDirectory （Identity Manager 中 Identity Vault 的基础）会频繁地记录请求信息，并将信息储存在索引中。对其特性已编制索引的对象运行复杂查询时，查询返回速度大大加快。

eDirectory 自带了以下已编制索引的特性：

```
Aliased Object Name cn dc Equivalent to Me extensionInfo Given Name
```

```
GUID ldapAttributeList ldapClassList Member NLS: Common Certificate
Obituary Reference Revision Surname uniqueID uniqueID_SS
```

安装 Identity Manager 时，将使用新的对象类类型和属于用户应用程序的新特性扩展默认目录纲要。默认情况下，特定于用户应用程序的特性不会编入索引。为了实现更佳的性能，您会发现将其中一些特性 （可能还有一些传统的 LDAP 特性）编入索引会非常有用，特别是在用户树枝包含 5,000 个以上的对象的情况下。

一般的想法是仅对已知需定期查询的特性编制索引。 （不同生产环境中也完全可能是不同的特性。）确认哪种特性使用率更高的唯一方法是收集运行时谓词统计数字。 （但是，收集过程本身也会导致性能下降。）

《eDirectory 管理指南》中对收集谓词统计数字的过程进行了详细介绍。该处也对索引进行更详细的介绍。通常，需要进行以下操作：

- 使用 Console One 打开感兴趣的特性的谓词统计数字集合
- 使系统处于负载状态
- 禁用统计数字集合，并分析结果
- 为每种可能从索引中受益的特性创建索引

如果已知道要对哪种特性编制索引，则不必使用 Console One。可以通过 《eDirectory 维护》 > 《索引》在 iManager 中创建并管理索引。例如，如果知道组织结构图中的用户将很可能基于 *isManager* 特性执行搜索，可以尝试对该特性编制索引，以查看性能是否得到增强。

注释：最好的做法是至少为 *manager* 和 *isManager* 特性编制索引。

有关对特性编制索引和性能的深入讨论，请参见 Peter Kuo 和 Jim Henderson 编写的 《*Novell eDirectory* 查错指南》中的 《调节 eDirectory》章节 （QUE Books， ISBN 0-7897-3146-0）。

也可参见主要的 《*eDirectory* 管理指南》中的 《维护 Novell eDirectory》章节 （其中包括性能调节指导）。

2.3.3 JVM

分配到 Java 虚拟机的内存堆内存的数量会影响性能。如果指定的最小或最大内存值过低或者过高 （过高意味着超过了计算机的物理内存），页文件交换可能会过多。

通过在文本编辑器中编辑 [IDM]/jboss/bin/ 下的 run.conf 或 run.bat 文件 （前者适用于 Linux，后者适用于 Windows），可以设置 JBoss 服务器的最大 JVM 大小。将 《-Xmx》从 *128m* 增加到 *512m*，或者更高。可能需要一些试验来确定特定环境的最佳设置。

注释：可以在 http://wiki.jboss.org/wiki/Wiki.jsp?page=JBossASTuningSliming (http://wiki.jboss.org/wiki/Wiki.jsp?page=JBossASTuningSliming) 中找到 JBoss 和 Tomcat 性能调节提示。

2.3.4 会话超时值

可以在 *IDM.war* 存档的 *web.xml* 文件中更改会话超时 （在服务器引起会话超时的警告对话框出现之前，万维网浏览器中的页面处于无人值守状态的时间量）。应该调节该值以使服务器与应用程序要运行的使用环境相匹配。一般情况下，建议尽量减少会话超时。如果业务要

求可以接受 5 分钟的会话超时，则与超时值为 10 分钟相比，服务器释放未使用的资源的速度可提高一倍。这将使得万维网应用程序具有更高的性能和可伸缩性。

调整会话超时时，请考虑以下问题：

- 如果短时间内有很多用户登录，则较长的会话超时可能导致 JBoss 服务器内存用尽。对于任何打开会话过多的应用程序服务器都是如此。
- 用户登录到用户应用程序时，将为该用户创建 LDAP 连接并与会话联结。因此，打开的会话越多，保持的 LDAP 连接数目就越多。会话超时越长，保持的连接打开的时间越长。 LDAP 服务器的打开连接过多 （即使为空闲连接）可能会导致系统性能降低。
- 如果服务器开始出现 OutOfMemoryErrors，并且已对服务器和使用环境的 JVM 内存堆和垃圾收集调节参数进行了最佳调节，那么应考虑缩短会话超时。

要调整会话超时值，需要打开 *IDM.war* 存档，在其中查找 *web.xml* 文件，并编辑文件的以下部分 （特别是此处显示为 20 （表示 20 分钟）的数字值，该值为默认值）：

```
<session-config>     <session-timeout>20</session-timeout> </session-
config>
```

然后需要保存文件和存档，并重启动服务器。

注释：最好由熟悉 Java 万维网应用程序开发和部署的人员进行万维网存档文件手动编辑。

2.4 群集

在群集环境中使用用户应用程序时必须考虑三件事情：

- JBoss 群集配置 （请参见 “群集 JBoss”在第 40 页 ）
- 用户应用程序超速缓存配置 （请参见 “配置用户应用程序群集组超速缓存配置”在第 44 页 ）
- 工作流程引擎配置 （请参见 “配置群集的工作流程”在第 44 页 ）

2.4.1 群集 JBoss

群集是提供一组服务的应用程序服务器节点的集合。使用群集的目的是提高应用程序的性能和可靠性。一般而言，群集为企业应用程序提供三个关键益处：

- 高可用性
- 可伸缩性 （容量更大）
- 负载平衡

高可用性意味着应用程序在部署期间的大部分时间内都可靠并且可用。因为在所有节点上运行同一应用程序，所以群集能提供高可用性。如果一个节点失败，则应用程序仍将在其它节点上运行。在群集中运行时， Identity Manager 用户应用程序将获得较高的可用性。但是，Identity Manager 用户应用程序不支持 HTTP 会话复制。这意味着如果在某节点上进行会话时该节点失败，会话信息将会丢失。

负载平衡是在群集成员中分发工作量的做法。负载平衡的目的是提高性能。可以通过多种方法实现负载平衡 （例如， DNS 循环复用、硬件负载平衡）。有关各种负载平衡方法的讨论，

请参见 http://www.onjava.com/pub/a/onjava/2001/09/26/load.html (http://www.onjava.com/pub/a/onjava/2001/09/26/load.html)。无论选择何种方法，都将要在群集配置中包含负载平衡。

JBoss 群集组

JBoss 群集以名为 JGroups 的通讯模块为基础。JGroups 与 JBoss 一起安装 （也可以在没有 JBoss 的情况下单独使用）。JGroups 可提供组之间的通讯，这些组共享常用名、多路广播地址以及多路广播端口。

安装群集 JBoss 服务器时， JBoss 将定义两个不同的 JGroups 组，用于管理群集。一个组为 *DefaultPartition*，在 /deploy/cluster-service.xml 中定义。 JBoss 使用此群集组提供核心群集服务。JBoss 还定义了另一个名为 *Tomcat-Cluster* 的群集组。此群集组在 /deploy/tc-cluster-service.xml 中定义。此群集组为 JBoss 内运行的 Tomcat 服务器提供会话复制。

Identity Manager 用户应用程序使用第三个群集组。此群集组使用 UUID 名以尽量减少与其它群集组 （用户可能将其添加到服务器中）冲突的风险。默认情况下，此群集组名为 c373e901aba5e8ee9966444553544200。此群集未使用 JBoss 服务文件进行配置。配置设置位于目录中，可以使用用户应用程序管理功能进行配置。如果熟悉 JGroups 和 JBoss 群集，则可以使用此界面调整用户应用程序群集配置。重启动服务器节点后，对该节点的群集配置所做的更改才能生效。

用户应用程序群集组仅用于在群集环境中协调用户应用程序超速缓存。它独立于两个 JBoss 群集组，并且不以任何方式与之进行交互。默认情况下，用户应用程序群集组和两个 JBoss 组使用不同的组名、多路广播地址和多路广播端口，因此无需进行重配置。

共享目录配置的所有 Identity Manager 3 应用程序都可共享用户应用程序群集组设置。管理员可使用用户应用程序管理界面中的本地设置选项从群集中去除节点，或更改群集中服务器的成员资格。例如，可以全局禁用群集，然后在本地对共享目录配置的服务器的子集启用该群集。

应用程序场

JBoss 允许将应用程序 EAR、 WAR 或 JAR 复制到一个群集 JBoss 实例的 farm 目录中，从而在群集中进行热部署。当群集正在运行时，在一台计算机上进行热部署将导致在此群集中所有实例上自动部署该部件。

由于 JBoss Application Server 4.0.2 版在使用方面存在未解决的问题，因此不推荐对它采取这种方式的应用程序部署。在编写本文档时，此版本已包含在用户应用程序安装程序中。但是，我们还是提供了使用 JBoss 场技术成功部署用户应用程序应执行的基本步骤 （请参见“使用 JBoss 场将用户应用程序部署到群集中”在第 44 页），因为此文档发布之后，该技术可能会改进。

MySQL 数据库

用户应用程序安装程序安装 MySQL 数据库管理器并创建用户应用程序使用的数据库，或者使用现有 Oracle、Microsoft SQL 服务器或 MySQL 数据库。数据库负责保证数据的持续性。JBoss 群集中的所有节点必须访问同一数据库实例。用户应用程序使用标准 JDBC 调用来访问并更新此数据库。用户应用程序使用联结到 JNDI 树的 JDBC 数据源打开与数据库的连接。如果使用用户应用程序安装程序创建 JBoss 群集，将安装数据源。如果选择手工安装 JBoss 群集，需要将数据源文件 (IDM-ds.xml) 复制到群集中所有节点的部署目录中。另外，如果要使用 MySQL，则需要将位于 JBoss/server/IDM/lib 目录中的 MySQL JDBC 驱动程序 (*mysql-connector-java-3.1.10-utf8-clob-fix-bin.jar*) 复制到 JBossserver/IDM/lib 目录中。

日志记录

要启用群集的日志记录，需要编辑 log4j.xml 配置文件，该文件位于 JBoss 服务器配置的 \conf 目录中 （例如， \server\IDM\conf），并取消底部的注释，如下所示：

```
<!--  Clustering logging --> - <!-- Uncomment the following to redirect
the org.jgroups and org.jboss.ha categories to a cluster.log file.
<appender name="CLUSTER"
class="org.jboss.logging.appender.RollingFileAppender"> <errorHandler
class="org.jboss.logging.util.OnlyOnceErrorHandler"/> <param
name="File" value="${jboss.server.home.dir}/log cluster.log"/> <param
name="Append" value="false"/> <param name="MaxFileSize" value="500KB"/
> <param name="MaxBackupIndex" value="1"/> <layout
class="org.apache.log4j.PatternLayout"> <param
name="ConversionPattern" value="%d %-5p [%c] %m%n"/> </layout> </
appender> <category name="org.jgroups"> <priority value="DEBUG" />
<appender-ref ref="CLUSTER"/> </category> <category
name="org.jboss.ha"> <priority value="DEBUG" /> <appender-ref
ref="CLUSTER"/> </category> -->
```

可以在 JBoss 服务器配置的 *log* 目录中找到 *cluster.log* 文件 （例如， *\server\IDM\log*）。

2.4.2 将用户应用程序安装到 JBoss 群集

将用户应用程序安装到群集的推荐方法是，使用用户应用程序安装程序将用户应用程序安装到群集中的每个节点。虽然不建议使用 JBoss 场将用户应用程序部署到群集中，但本文中也包括了这种方式的操作过程，供您选用。

在群集中的每个节点上使用用户应用程序安装程序

JBoss 附带了三种现成的服务器配置：最小、默认和所有。只有在所有配置中可以启用群集。/deploy 文件夹中的 cluster-service.xml 文件说明默认群集分区的配置。如果安装用户应用程序时指示安装程序要安装到群集中，安装程序将生成所有配置的拷贝，将拷贝命名为 *IDM* （默认情况下为此名称；安装程序允许更改拷贝名称），并将用户应用程序安装到此配置中。

要使用用户应用程序安装程序将用户应用程序安装到群集中的每个节点，请执行以下操作：

1 在第一个 JBoss 节点上完整安装用户应用程序 （MySQL、 JBoss 以及用户应用程序）。有关使用用户应用程序安装程序的信息，请参见 《*Identity Manager 3* 安装指南》。
- 如果要使用 MySQL 作为用户应用程序的数据库，则用户应用程序安装程序将创建 MySQL 的新安装。请记住所指定的 MySQL 根用户口令；在群集中的其余节点上安装用户应用程序时需要此信息。
- 在安装程序 《IDM 配置》屏幕中，选择 " 群集 （所有） " 选项。
- 选择其它适合于环境的安装选项。

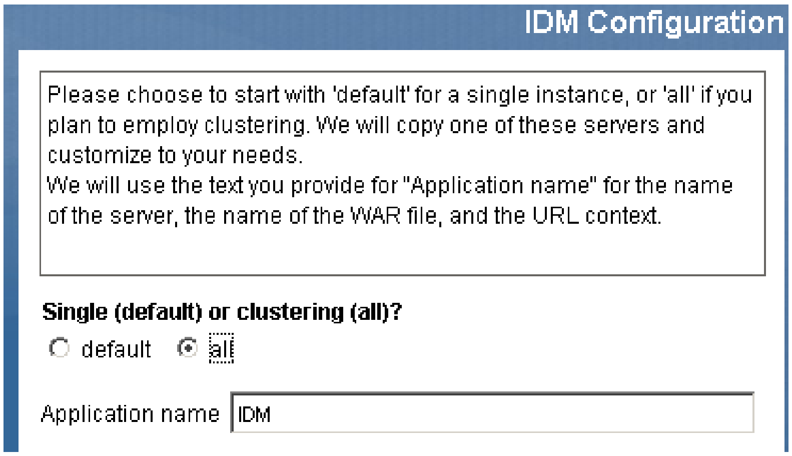
2 如果尚未运行 MySQL，则使用位于 /IDM/mysql 目录中的 *start-mysql.bat* 文件启动 MySQL。

注释 **:** 在 Linux 中，以下壳层命令有助于确定是否正在运行 MySQL 守护程序：

```
ps -A | grep mysqld
```

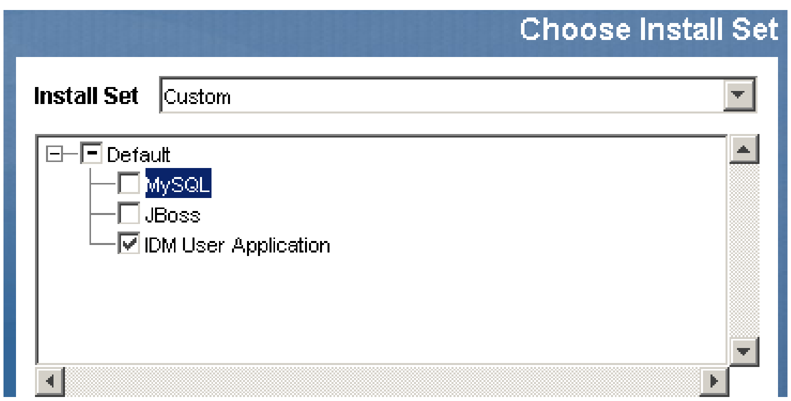
如果此命令返回多个以 mysqld 结束的行，那么此守护程序正在运行。

3 使用位于 *IDM* 目录中的 *start-jboss.bat* (Windows) 或 *start-jboss.sh* (Linux) 文件启动 JBoss 和用户应用程序。



4 在 JBoss 群集中的每个附加节点上执行用户应用程序的自定义安装。

- 仅选择要安装的用户应用程序：



- 指定将安装用户应用程序数据库的服务器的 IP 地址或主机名。
- 指定用户应用程序数据库的数据库用户名和口令。如果使用 MySQL，用户名为 root，口令为步骤 1 中的安装进程期间所指定的口令。
- 在安装程序 《IDM 配置》屏幕中，选择 " 群集 （所有） " 选项。
- 选择其它适合于环境的安装选项。

5 使用位于 *IDM* 目录中的 *start-jboss.bat* (Windows) 或 *start-jboss.sh* (Linux) 启动 JBoss 群集中每个节点。

使用 **JBoss** 场将用户应用程序部署到群集中

请勿在 JBoss 4.0.2 版或更早版本中使用 JBoss 场，可能会遇到问题 （请参见 http://jira.jboss.com/jira/browse/JBAS-1899 (http://jira.jboss.com/jira/browse/JBAS-1899)）。建议使用用户应用程序安装程序在群集中的每个节点上安装用户应用程序 （请参见本章中的 “在群集中的每个节点上使用用户应用程序安装程序”在第 42 页 ）。但是，如果要使用场将用户应用程序部署到使用 JBoss 4.0.3 或更高版本的 JBoss 群集中，请遵循以下步骤。

注释 **:** 这些步骤针对希望独自试用 JBoss 4.0.3 的客户。正式支持的版本为 4.0.2。

要使用 JBoss 场将用户应用程序部署到群集中，请执行以下操作：

1. 选择要安装的用户应用程序和 MySQL （如果使用 MySQL 的话；否则，将只安装用户应用程序），将用户应用程序自定义安装到 JBoss 群集的一个节点上。执行安装时此节点上的所有群集都可运行，但是安装用户应用程序的节点应该是群集中第一个启动的节点。
2. 将位于 /server/IDM/lib 目录中的 JDBC 驱动程序文件 （例如，如果要使用 MySQL，JDBC 驱动程序为 *mysql-connector-java-3.1.10-utf8-clob-fix-bin.jar*）复制到群集中每个节点的相应目录中。
3. 将随用户应用程序一起安装的 JRE 的 /lib/security 目录中的 *cacerts* 文件复制到群集中各个节点的 JRE/lib/security 目录中。
4. 将 IDM.war 文件和 IDM-ds.xml 数据源文件从服务器配置目录的 /deploy 目录移动到服务器配置目录的 /farm 目录。必须实际移动这些文件。不要将原文件留在 /deploy 目录中。
5. 启动用户应用程序的数据库 （如果要使用所提供的 MySQL，请用位于 /IDM/mysql 目录中的 *start-mysql.bat* 文件启动 MySQL）。
6. 使用 *start-jboss.bat* (Windows) 或 *start-jboss.sh* (Linux)（位于安装了用户应用程序和用户应用程序数据库的节点上的 *IDM* 目录中）启动 JBoss 和用户应用程序。
7. 启动群集中的其它节点。

2.4.3 配置用户应用程序群集组超速缓存配置

熟悉 JGroups 和 JBoss 群集的用户可以使用用户应用程序管理用户界面修改群集组超速缓存配置 （请参见 “群集的超速缓存设置”在第 205 页 ）。重启动服务器节点后，对该节点的群集配置所做的更改才能生效。

2.4.4 配置群集的工作流程

工作流程引擎群集独立于用户应用程序超速缓存框架工作。必须执行若干步骤以确保工作流程引擎在群集环境中的正常工作。

- 群集中的所有服务器都需指向同一数据库。如果使用推荐的方法将用户应用程序安装到群集中 （请参见 “在群集中的每个节点上使用用户应用程序安装程序”在第 42 页 ），则在安装进程期间，通过指定安装用户应用程序数据库的服务器的 IP 地址或主机名，可以完成此操作。如果使用场将用户应用程序部署到群集节点中 （请参见 “使用 JBoss 场将用户应用程序部署到群集中”在第 44 页 ），将数据源文件 (IDM-ds.xml) 从首次安装用户应用程序的节点上的 /deploy 目录移动到 /farm 目录中，即可完成此操作。这将导致数据源被部署到群集中的所有节点上。

- 需要使用唯一的引擎 ID 启动群集中的每个服务器。可以在启动服务器时通过设置 *com.novell.afw.wf.engine-id* 系统属性完成此操作。例如，如果要启动 JBoss 并将引擎 ID ENGINE1 指派给该服务器的工作流程引擎，应使用以下命令：

  run.sh -Dcom.novell.afw.wf.engine-id=ENGINE1 (Linux)

  run.bat -Dcom.novell.afw.wf.engine-id=ENGINE1 (Windows)

一个工作流程进程实例由特定服务器上运行的工作流程引擎启动后，就只能在该服务器上运行并完成。这将确保工作流程进程的安全执行。但是，它不提供进程实例故障转移支持。如果群集中的服务器崩溃，则直到重启动具有同一 ID 的引擎后，进程实例才会重启动。

如果因严重的硬件或软件故障而无法重启动服务器计算机，则可以使用那台不可恢复的计算机上所用的同一工作流程引擎 ID，在新计算机上启动应用程序服务器。由于引擎 ID 是一个逻辑名，而不是对引擎所运行的物理计算机的直接映射，因此中断的进程实例将在新计算机上成功完成。

进程实例由启动进程的引擎所拥有。但是，用户可以登录群集中的任意用户应用程序以查看进程详情、收回进程或完成所指派的任务。收回的进程或在并未拥有此进程的引擎上完成的任务将进入待发状态，一旦被拥有它们的引擎发现，将继续执行。

配置用户应用程序环境

II

以下章节说明如何配置 Identity Manager 用户应用程序环境的各个方面，以满足组织的需要。

配置用户应用程序驱动程序 3

3.1 关于用户应用程序驱动程序

用户应用程序驱动程序负责启动供应工作流程，并负责将 Identity Vault 中所做的更改通知用户应用程序 （例如，当使用 Designer for Identity Manager 对目录提取层进行更改时）。此驱动程序仅使用订购者通道。此驱动程序处理从 Identity Vault 到应用程序服务器上运行的用户应用程序的讯息。虽然用户应用程序中发生的某些事件会被报告回 Identity Vault，但这些事件并不经过该用户应用程序驱动程序的发布者通道。

启动应用程序服务器时，此驱动程序将与应用程序服务器建立会话。此驱动程序会将讯息发送至应用程序服务器上运行的用户应用程序 （例如， " 检索一组新的虚拟目录定义 "）。

驱动程序的源代码组件包括：

- ComposerDriverShim.jar – 编辑器驱动程序 Shim。安装在 *lib* 目录 *\Novell\NDS\lib* (Windows) 或 *classes* 目录 */usr/lib/dirxml/classes* (Linux) 中
- srvprvUAD.jar – 应用程序驱动程序 Shim。安装在 *lib* 目录 *\Novell\NDS\lib* (Windows) 或 *classes* 目录 */usr/lib/dirxml/classes* (Linux) 中
- UserApplicationDriver.xml - 包含用于安装新驱动程序的预配置数据的文件。安装在 *DirXML.Drivers* 目录 *\Tomcat\webapps\nps\DirXML.Drivers* (Windows) 或 */usr/lib/dirxml/rules/DirXML.Drivers* (Linux) 中

用户应用程序驱动程序组件是在安装 Identity Manager 3 时进行安装的。在运行 Identity Manager 3 用户应用程序之前，必须将用户应用程序驱动程序添加到新的驱动程序集或现有的驱动程序集中，并激活该驱动程序。

根据工作环境的不同，可能只需要对用户应用程序驱动程序进行少量配置，也可能需要在驱动程序策略中实施一组复杂的业务规则。与其它 Identity Manager 驱动程序一样，用户应用程序驱动程序进行数据同步时的机制也很灵活。

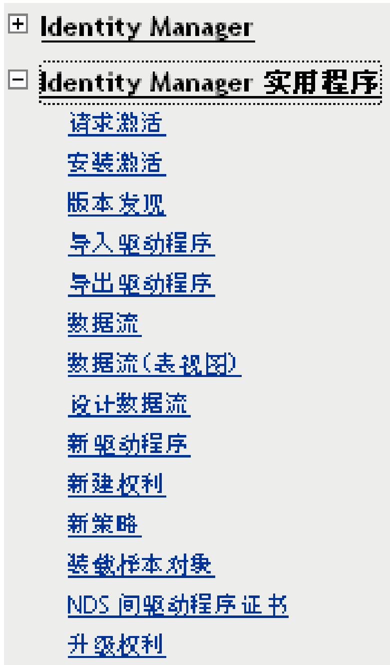
本章说明如何创建、配置和启动用户应用程序驱动程序，以及如何配置驱动程序，以根据 Identity Vault 中的事件自动触发工作流程。其中包含以下几节：

3.2 创建用户应用程序驱动程序

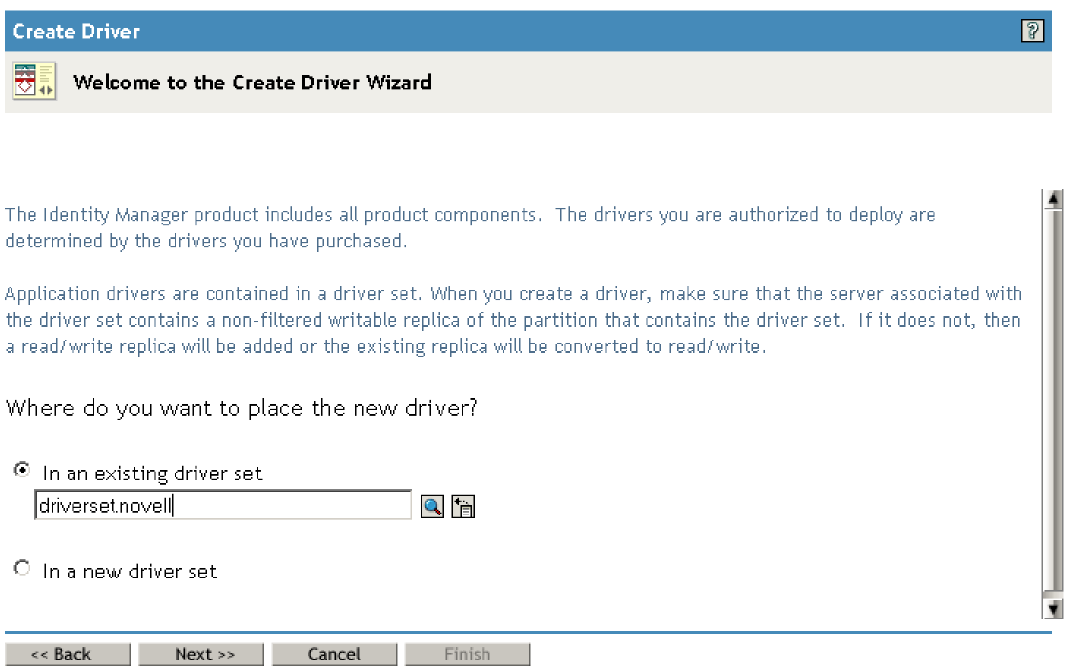
要创建此驱动程序，请执行以下操作：

1 登录到管理 Identity Vault 的 iManager 实例中。

2 打开 iManager 导航框架中的 《Identity Manager 实用程序》节点。



3 单击 《新驱动程序》。将显示 《创建驱动程序》向导：

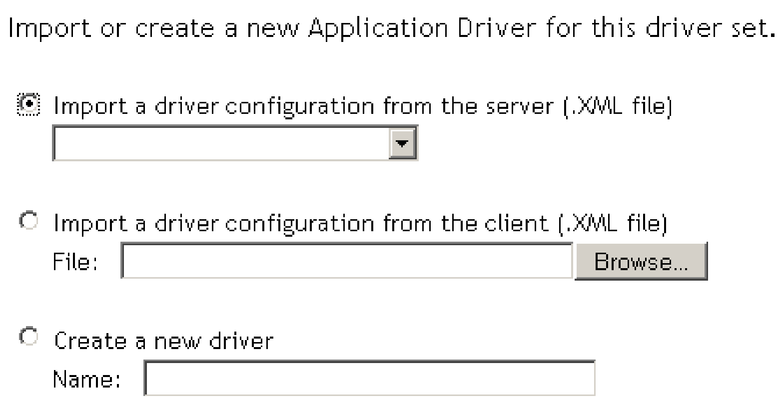


下一步是选择创建新驱动程序的位置。可以在现有的驱动程序集中创建驱动程序，或创建新的驱动程序集。

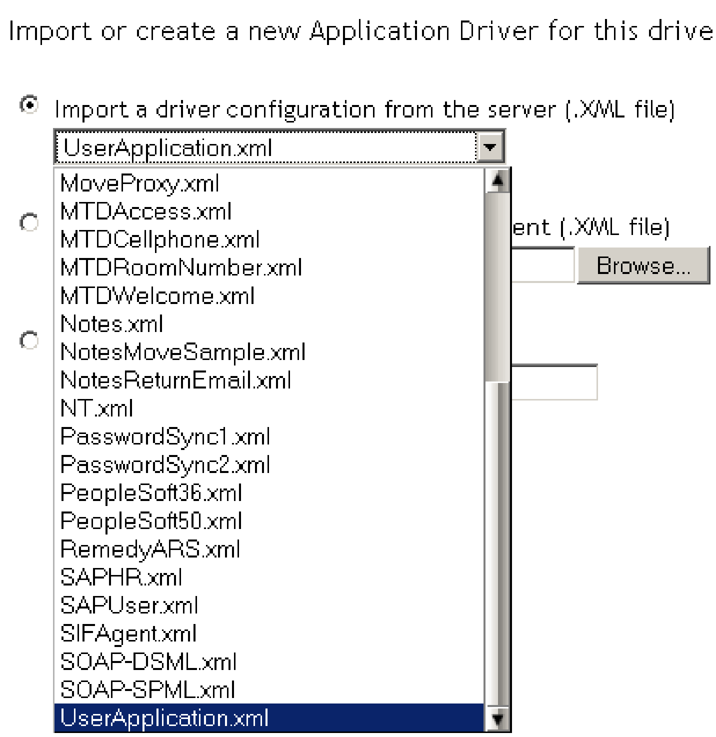
4 如果选择 《在现有驱动程序集中》，将出现一个向导，通过该向导可以浏览 Identity Vault，找到此驱动程序集。选择现有驱动程序集，然后选择 《下一步》。

如果选择 《在新驱动程序集中》，将显示一个屏幕，通过该屏幕可以定义新驱动程序集的属性。为驱动程序集指定名称、树环境以及服务器，然后选择 《下一步》。

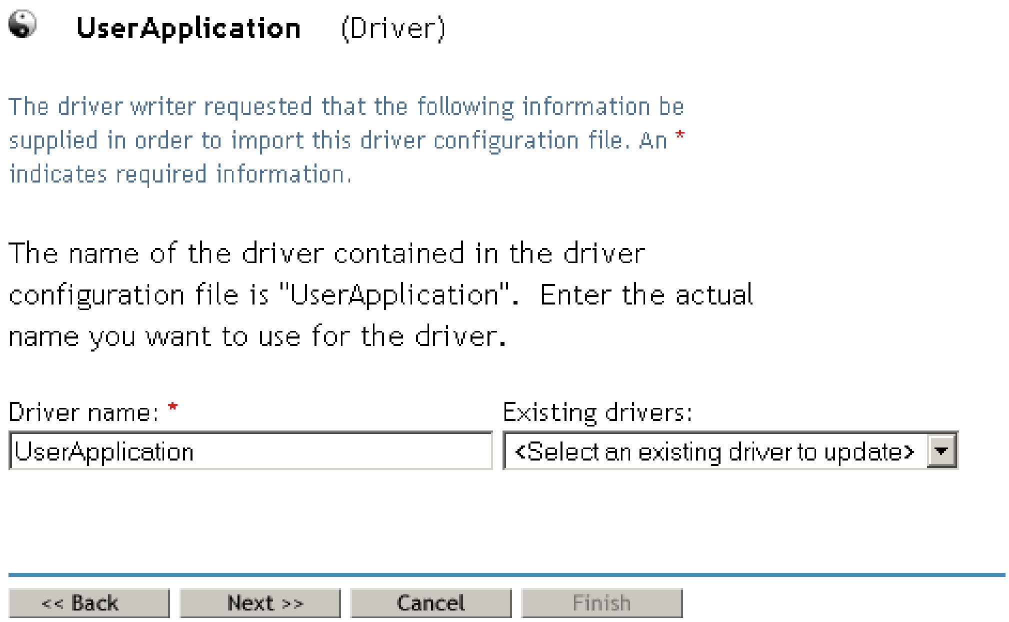
将显示 《创建驱动程序》向导的下一个屏幕：



5 单击 *Import a driver configuration from the server* （从服务器中导入驱动程序配置）选项，然后从 XML 文件列表中选择 *UserApplication.xml*：



6 单击 《下一步》。 《创建驱动程序》向导将显示一个页，可以在其中命名并配置驱动程序：



驱动程序的默认名称为 UserApplication。可以使用此默认名称，也可以针对项目选择更有意义的名称。

7 如有必要，请在 《驱动程序名》字段中键入驱动程序的新名称。

8 在 《鉴定 ID》字段中，使用点格式 （例如， admin.orgunit.novell）指定用户应用程序管理员的 DN （有关用户应用程序管理员的说明，请参见 "用户应用程序管理员"在第 15 页 ）。

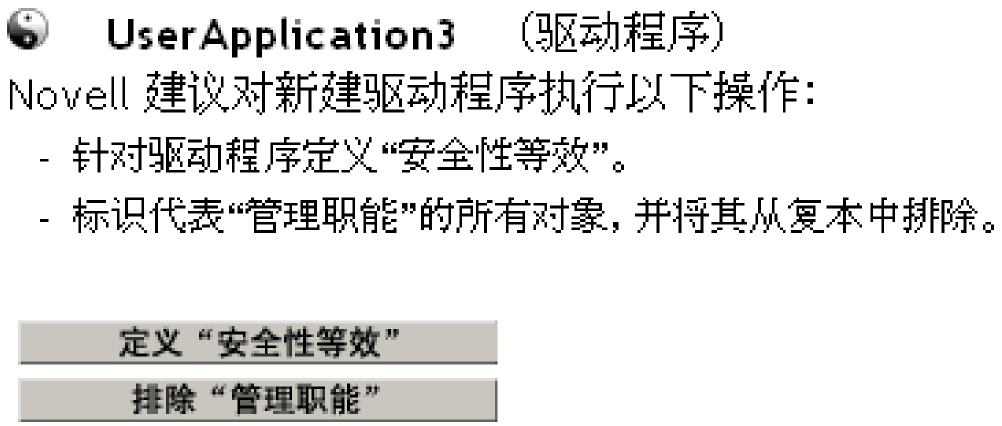
9 在 《应用程序口令》字段和 《再输入口令》字段中，为 《鉴定 ID》字段中标识的用户应用程序管理员指定口令。

10 在 《应用程序环境》字段中，键入安装用户应用程序时指定的应用程序名称。默认名称为 IDM。

11 在 《主机》字段中，指定用户应用程序所运行的应用程序服务器的主机名或 IP 地址。

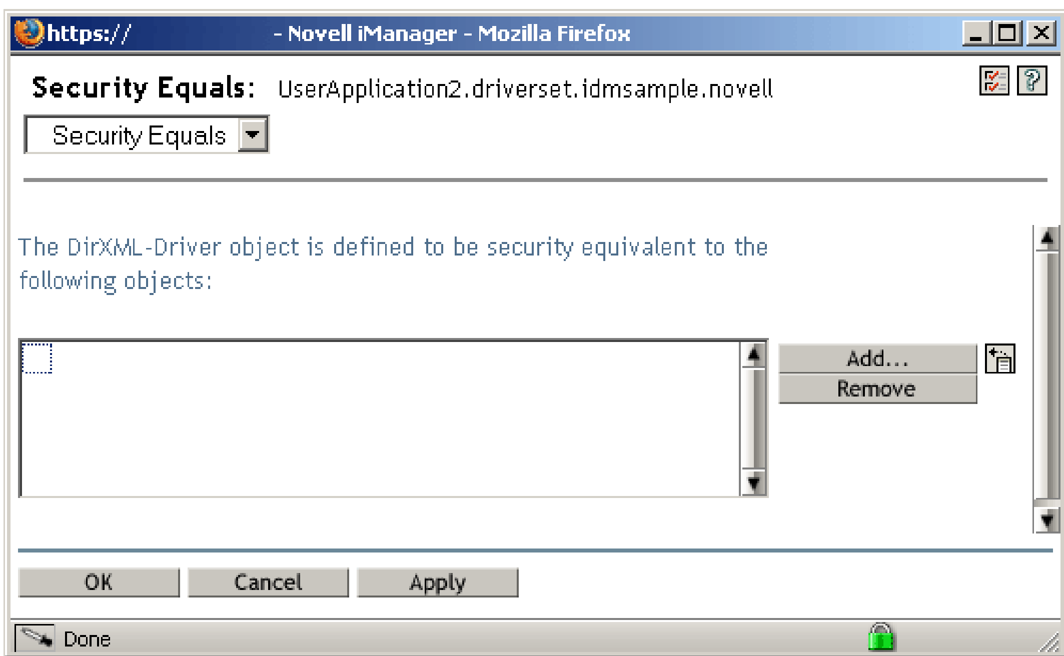
12 在 《端口》字段中指定端口 （例如 8080），驱动程序将在该端口与应用程序服务器中运行的用户应用程序进行通讯。

13 单击 《下一步》。将显示一条讯息，指示正在导入驱动程序配置，然后将显示 《创建驱动程序》向导的下一页。

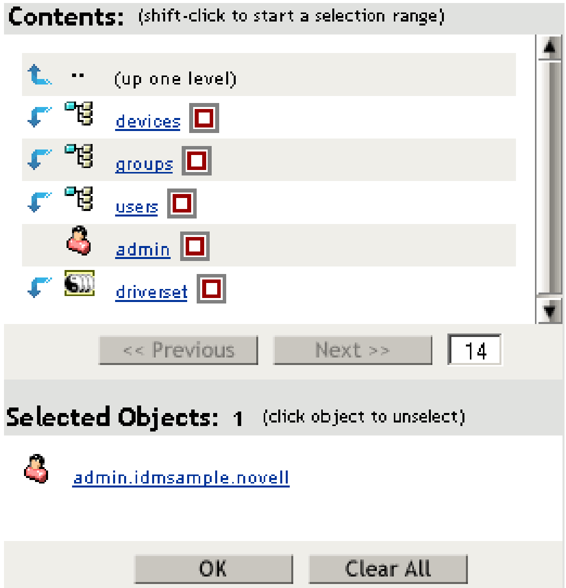


必须为驱动程序对象授予足够的 Identity Vault 权限，使其可以对任何对象进行读或写。可通过授予驱动程序对象 《安全性等效》来完成此操作。驱动程序必须对用户、邮局、资源和分发列表具有读 / 写访问权限，并对邮局树枝具有创建、读以及写权限。通常应为此驱动程序授予与 Admin 相等的安全性。

14 单击 《定义安全性等效》。将显示新窗口：



15 单击 《添加》。将显示一个窗口，可以在此窗口中选择树中的某一对象，该对象具有要指派给此驱动程序的相应权限级别 （例如， admin）：



16 从树中选择具有 Identity Vault 所需权限级别的对象，然后单击 《确定》。将返回上一个窗口。

17 单击 《确定》。将返回 《创建驱动程序》向导。

18 单击 *Exclude Administrative Roles* （排除管理职能）。将显示 《排除的用户》窗口。使用此功能可防止将管理员口令在其它 Identity Vault 中所做的更改复制回此驱动程序所属的树时，管理员被封锁在用户应用程序驱动程序之外。

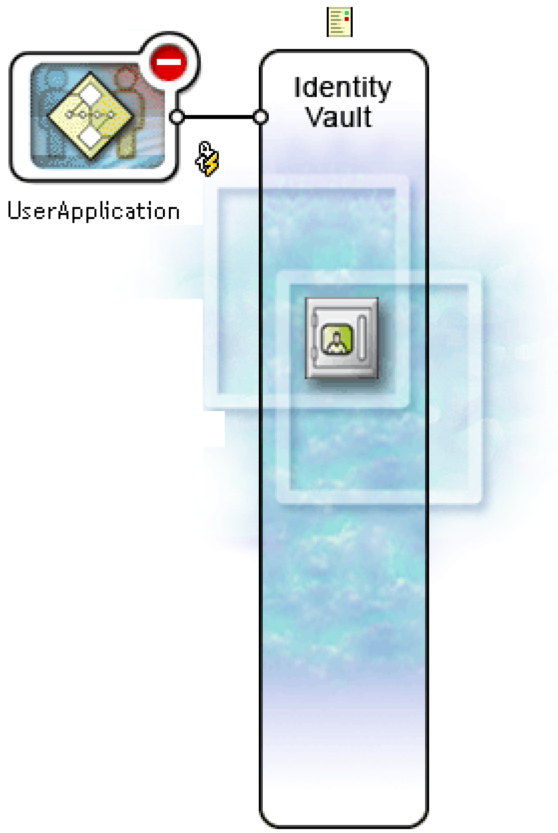
19 单击 《添加》。将显示一个窗口，可以在其中浏览目录树，以查找不允许将其数据传递到驱动程序的用户。通常会排除 Admin 对象，因为在多数情况下，跨驱动程序连接复制这些对象的数据不是一种好的做法。

20 选择要排除的管理职能，然后单击 《确定》。将返回上一个窗口。

21 单击 《确定》。将返回 《创建驱动程序》向导。

22 单击 《下一步》。将显示驱动程序摘要页。

23 单击 《完成概述》。在 Identity Vault 中将显示该驱动程序的图形表示形式：



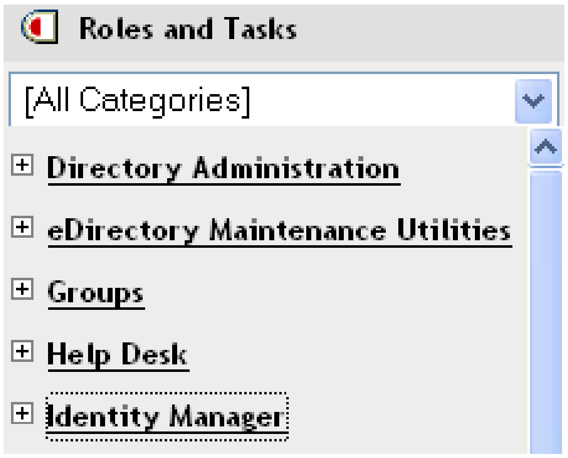
注释 **:** 使用 iManager 导航树中 *Identity Manager* 下的 《Identity Manager 概述》链接，可以随时再次查看此屏幕。

新驱动程序显示为与 Identity Vault 主干连接的大图标。

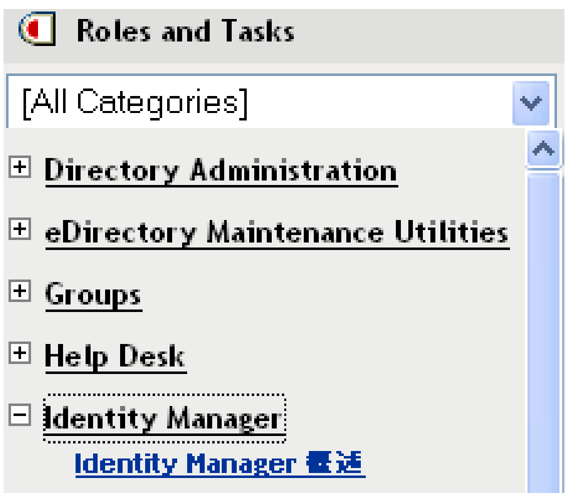
3.3 启动用户应用程序驱动程序

要启动用户应用程序驱动程序，请执行以下操作：

1 单击 iManager 导航树中的 *Identity Manager* 链接，以查看 Identity Manager 类别中可用的命令：



2 单击 iManager 导航树中 *Identity Manager* 链接下的 《Identity Manager 概述》链接：



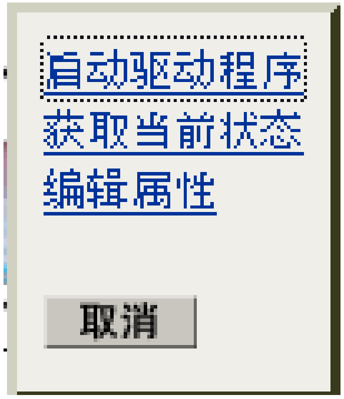
将显示向导，通过该向导可以浏览系统并找到驱动程序集，其中包含要激活的驱动程序。

3 选择驱动程序集，然后单击 《下一步》。将显示 《Identity Manager 概述》页。

4 单击驱动程序图标右上角的圆形状态指示器：



将显示一个菜单，其中列出了用于启动和停止驱动程序以及编辑驱动程序属性的命令：



5 单击 《启动驱动程序》。

3.4 设置要自动启动的工作流程

如果安装了预置模块，当用户通过请求资源启动供应请求时，工作流程将自动启动。另外，Identity Manager 用户应用程序驱动程序还可监听 Identity Vault 中的事件，进行相应配置后，它还能通过启动相应的供应工作流程对事件做出响应。例如，将新用户添加到 Identity Vault 中时，可以配置用户应用程序驱动程序以自动启动供应工作流程。可以使用 Identity Manager 策略和规则配置用户应用程序驱动程序，以自动启动工作流程。

3.4.1 关于策略

可以将过滤器和策略用于用户应用程序驱动程序，方法与将它们用于其它 Identity Manager 驱动程序的方法相同。当 Identity Vault 中发生某一事件时，Identity Manager 将创建描述该事件的 XML 文档。XML 文档将沿通道传递到已连接系统 （在这种情况下，已连接系统为用户应用程序）。使用与驱动程序关联的过滤器和策略，可以定义如何响应事件，以及在进程中如何将该 XML 文档转换为已连接系统所期望的格式。Identity Manager 提供多种类别的策略 （例如，事件转换、命令转换、纲要映射、输出转换），可以按规定的顺序应用这些策略转换 XML 文档。本节将提供一个示例，说明如何根据 Identity Vault 中的事件启动工作流程。任何策略都可用于触发工作流程，但此示例所演示的是一个最简便且最有用的方法。

创建用户应用程序驱动程序时，将创建一个事件转换策略以供驱动程序使用。事件转换策略负责创建将由其余订购者通道策略处理的 XML 文档。

注释：不要更改创建用户应用程序驱动程序时所创建的事件转换策略。此策略的 DN 以 Manage.Modify.Subscriber 开头。更改此策略可能导致工作流程进程失败。

还将创建一个空的纲要映射策略。可以使用此策略作为根据 Identity Vault 中的事件触发工作流程的起点。

3.4.2 设置一个根据 Identity Vault 中的事件启动的工作流程

自动启动工作流程最简单的方法是使用纲要映射策略编辑器，用户应用程序驱动程序为此提供了一个空策略以供编辑。

使用纲要映射策略编辑器可将 Identity Vault 特性 （包括 eDirectory *trigger* 特性，该特性发生更改时将启动工作流程）映射到目标工作流程的运行时数据。运行时数据由工作流程定义模板确定 （有关工作流程定义模板的信息，请参见第 22 章 “配置供应请求定义”在第 295 页 ）。运行时数据是成功完成工作流程所必需的。创建工作流程后，将在 Identity Vault 中创建大量的全局特性，这些特性可用于自定义用户应用程序驱动程序的行为。全局特性是不属于任何 Identity Vault 对象类的特性。这些特性为 <workflowName>_StartWorkflow、<workflowName>_recipient 和 <workflowName>_reason。还有两个特性始终存在，分别名为 AllWorkflows:reason 和 AllWorkflows:recipient。_StartWorkflow 特性用于启动工作流程。_recipient 和 _reason 特性用于从 Identity Vault 中接受工作流程所需的运行时数据。

在执行此过程之前，应该知道要用作工作流程触发器的 Identity Vault 特性的名称。还应该知道要启动的工作流程的名称。所有工作流程都包含一个名为 <workflowName>_StartApprovalFlow 的特殊特性。通过将所需的 eDirectory 特性映射到工作流程的 <workflowName>_StartApprovalFlow 特性，可将此工作流程配置为根据 Identity Vault 中的事件自动启动。

要将工作流程设置为根据 Identity Vault 中的事件启动，请执行以下操作：

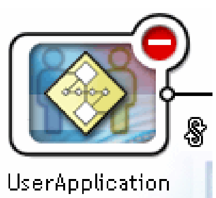
1 在 iManager 中，单击 iManager 导航树中 Identity Manager 下的 《Identity Manager 概述》链接。



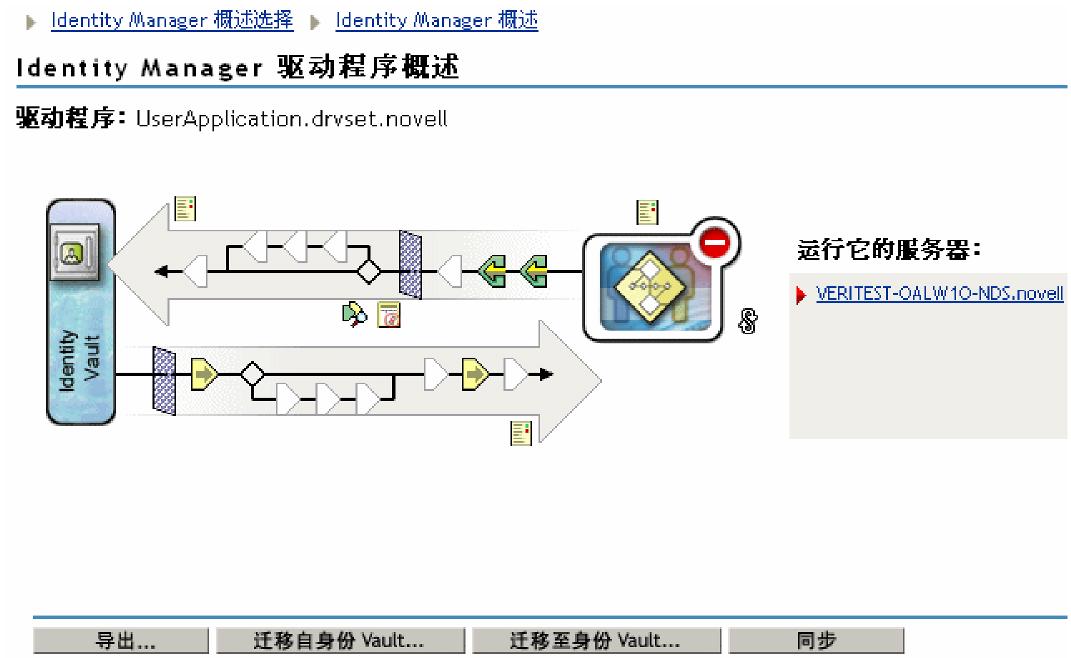
将显示 《Identity Manager 概述》页。在此页中提示选择一个驱动程序集。

2 单击 《搜索整个树》；然后单击 《搜索》。将显示 《Identity Manager 概述》页，其中包含的图形显示出当前选定的驱动程序集中的驱动程序。

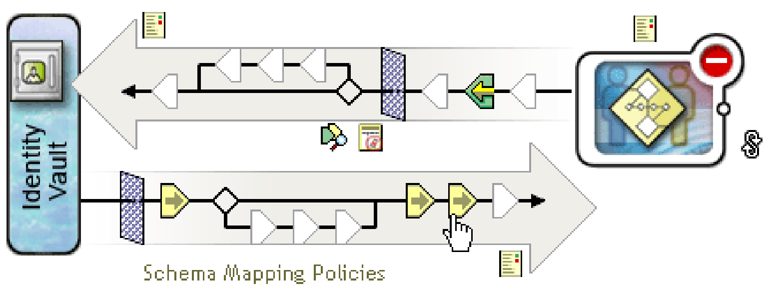
3 单击用户应用程序驱动程序的驱动程序大图标：



即显示 《Identity Manager 驱动程序概述》：



顶部的横向箭头表示发布者通道 （在用户应用程序驱动程序中不使用该通道），底部的横向箭头表示订购者通道。将鼠标指针移动到图形中的某个对象上时，将显示该对象的说明：



4 单击订购者通道的 《纲要映射策略》图标。即显示 《纲要映射策略》对话框，并突出显示默认纲要映射策略的名称：



5 单击《编辑》。即显示《Identity Manager 策略》对话框。此对话框用来将 Identity Vault 类映射到应用程序类。本过程不会使用到此功能。而是将 eDirectory 特性映射到全局用户应用程序特性。



6 单击 《刷新应用程序纲要》。将显示一条讯息，说明必须停止驱动程序以读取纲要，然后再重启动它。刷新纲要可能需要约 60 秒。此步骤会读取一组最新的工作流程信息，为下一步 （指定从 Identity Vault 移到将要启动的工作流程中的信息）做准备。

7 单击 《确定》刷新纲要。纲要刷新完成后将显示一条讯息。

8 单击 《确定》关闭纲要刷新讯息。返回到 《Identity Manager 策略》对话框。

9 单击 *Non Class Specific Attributes* （非特定类特性）。即显示 《Identity Manager 纲要映射策略编辑器》。



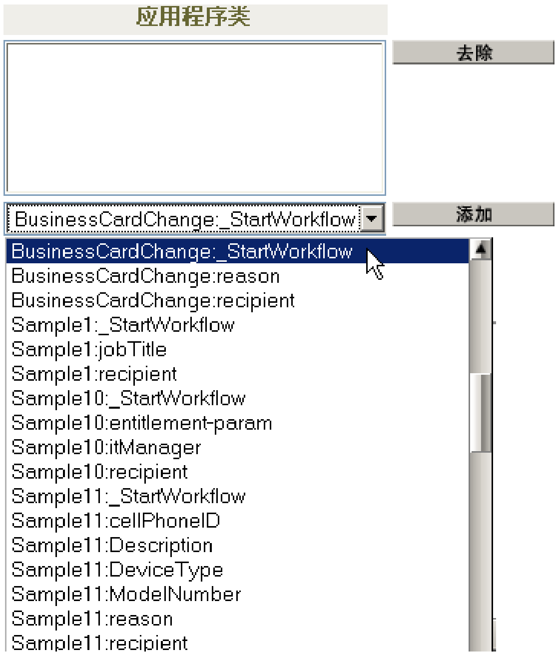
《eDirectory 特性》下拉列表中包含所有的 eDirectory 特性。

《应用程序特性》下拉列表中包含所有活动工作流程中的特性。列表中的特性以 AllWorkflows （表示该特性应用于所有工作流程）或特定工作流程的名称开头。如果要将同一个 eDirectory 特性 （如 manager）映射到所有工作流程的 manager 特性，可以将 manager 映射到 Allworkflows:manager。如果要将不同的 eDirectory 特性 （如 HRmanager）用于特定的工作流程，则可以将 eDirectory 特性映射到特定的工作流程特性 （如 BusinessCardChange:manager）。

已经映射的特性会并排显示在 《eDirectory 特性》和 《应用程序特性》列中。

在以下步骤中，我们将用于启动工作流程的 eDirectory 特性映射到该工作流程的 _StartWorkflow 特性。如果该工作流程还需要其它 eDirectory 特性，还应映射这些特性。例如，如果 eDirectory Address 特性是一个工作流程的触发器，而该工作流程可能还需要像 City 和 State 这样的特性。也可以将这些特性映射到策略中。

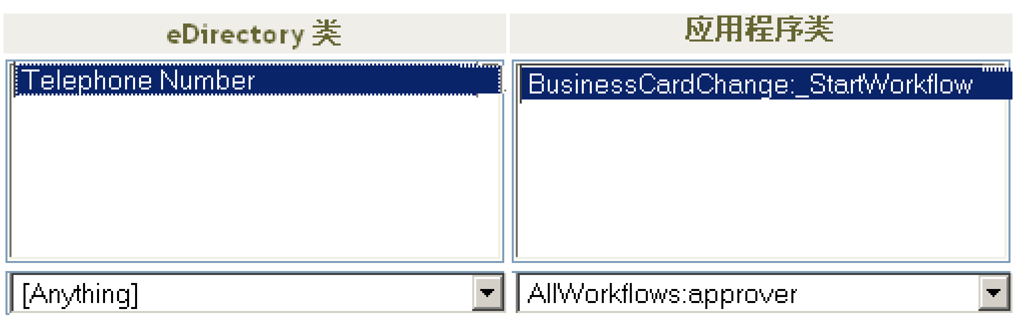
10 在《应用程序特性》列表中，选择要配置的工作流程的 _StartWorkflow 特性。下面的示例显示了 BusinessCardChange 工作流程的 _StartWorkflow 特性 (BusinessCardChange_StartWorkflow)。



11 在 《eDirectory 特性》列表中，选择某个 eDirectory 特性，在此特性发生更改时启动工作流程。在下面的示例中，选择了 Telephone 特性。这意味着只要员工的电话号码发生更改，就会启动 BusinessCardChange 工作流程。



12 单击 《添加》。此 eDirectory 特性即被映射到应用程序特性。



13 如果工作流程还需要其它 eDirectory 特性，请重复步骤 10 到步骤 12，直到映射了所有需要映射的特性。

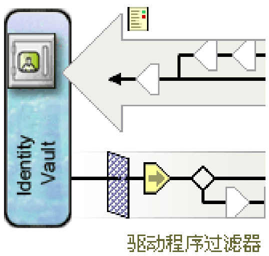
当映射到 application _StartApprovalFlow 特性的 eDirectory 特性发生更改时，工作流程将自动启动。但是，如果订购者通道驱动程序过滤器中包含此 eDirectory 特性，此 eDirectory 特性将仅到达纲要映射策略中。在以下步骤中，我们要将 eDirectory 特性添加到订购者通道驱动程序过滤器中

14 单击 《确定》关闭 《Identity Manager 纲要映射策略编辑器》。

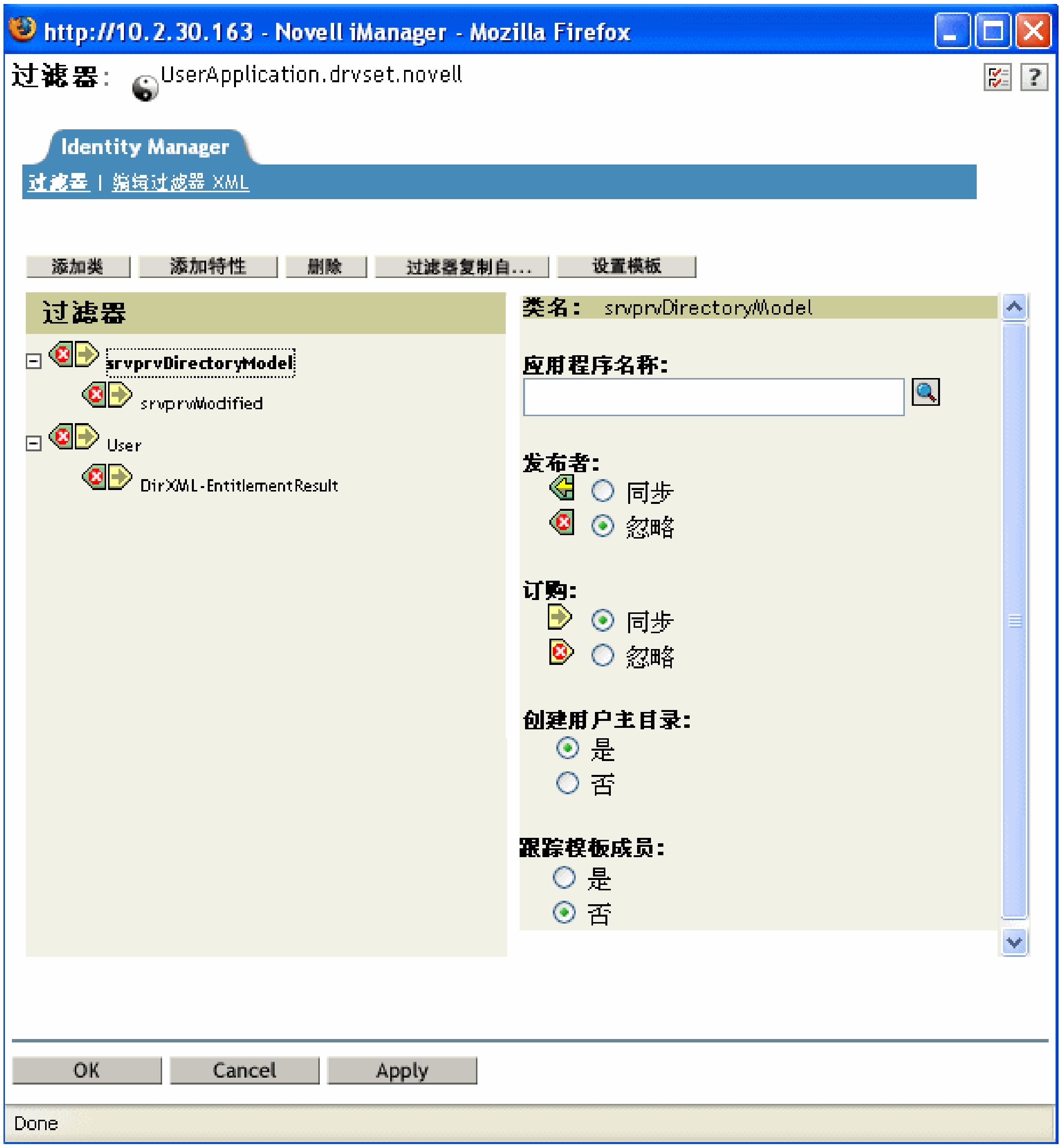
15 单击 《确定》关闭 《Identity Manager 策略》对话框。

16 单击 《关闭》以关闭 《纲要映射策略》对话框。

17 单击订购者通道的 《驱动程序过滤器》图标。



将显示过滤器窗口：



事件过滤器指定 Identity Manager 引擎为之处理事件的对象类和特性。左侧的只读 《过滤器》列表显示了类中的特性。右侧的 《类名称》列表显示了与目标对象关联的选项。

18 单击要添加到过滤器中的特性所属的类的名称 （如 User）。

19 单击 《添加特性》。即显示特性列表。

20 选择一个特性，然后单击 《确定》。此特性即被添加到 《过滤器》列表中。



21 单击该特性的名称。则在右侧面板中显示该特性的同步选项。



22 在 《订购》下方，单击 《同步》。



23 为此过滤器指定其它特性。如果希望报告和同步对特性值的更改，请为该特性选择《同步》。如果不希望报告和同步对特性值的更改，请选择 《忽略》。

24 单击 《确定》。将显示一条讯息，询问是否要重启动驱动程序以使更改生效。

25 单击 《确定》。即返回至 《Identity Manager 驱动程序概述》页。

配置目录提取层 4

本章说明如何使用目录提取层编辑器定义 Identity Manager 用户应用程序所用的目录提取层数据定义。包括以下主题：

4.1 关于目录提取层定义

目录提取层是一组数据定义，提供了 Identity Vault 的逻辑视图。目录提取层可定义：

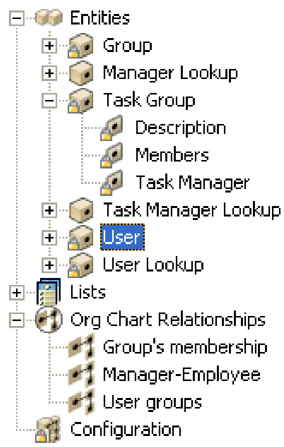
- 可在 Identity Manager 用户应用程序中使用的 Identity Vault 对象和特性。
- Identity Vault 数据在用户界面中的显示方式。
- 组织结构图入口小程序可以使用的关系。

如果要修改用户应用程序的外观或功能，可使用目录提取层编辑器来更改这些数据定义。可以通过以下操作进行更改：

- 添加其它 Identity Vault 对象
- 更改 Identity Vault 对象可用的特性集
- 更改列表内容
- 显示 Identity Vault 对象之间的不同关系

Identity Manager 用户应用程序安装过程会安装和部署用户应用程序正常运行所需的提取层定义的基集。此安装过程还将创建用户应用程序驱动程序和用户应用程序使用的 eDirectory 纲要扩展。有关这些纲要扩展的更多信息，请参见附录 A “纲要扩展”在第 335 页 。通过 Designer for Identity Manager 新建用户应用程序驱动程序实例时，将在本地文件系统中创建相同的文件基集。

必需的数据提取层数据定义 在开始自定义 Identity Manager 用户应用程序时，需要对目录提取层对象进行更改。但是，不能去除或更改某些 Identity Vault 对象 （称作实体）、特性、关系和列表，否则用户应用程序将不能正常运行。无法去除的定义由锁形图标标识。在本示例中，可以看到 Task Group 实体及其所有特性均已被锁定。



目录提取层定义的储存位置 目录提取层定义是 XML 文件，这些文件：

- 储存在本地设计程序计算机上的文件系统中，储存位置为供应项目的 Provisioning\AppConfig\DirectoryModel 子目录。如果项目中有多个用户应用程序，将会对目录名称进行编号。例如， AppConfig1、 AppConfig2 等。
- 部署到用户应用程序驱动程序的 AppConfig.DirectoryModel 树枝中。XML 文件储存在相应的目录提取层定义对象的 XMLData 特性中。每个实体、关系和列表都是包含在用户应用程序驱动程序的 AppConfig.DirectoryModel 树枝中的唯一对象实例。
- 超速缓存在部署用户应用程序的应用程序服务器中。

4.2 开始

使用 Designer for Identity Manager 供应视图和目录提取层编辑器的功能可以定义目录提取层的内容。请按以下步骤开始操作：

步骤	任务	说明
1	创建一个 Identity Manager 项目	其中包括： ◆ 配置 Identity Vault ◆ 指定驱动程序集属性 请参见 Identity Manager 文档。

步骤	任务	说明
2	将用户应用程序驱动程序添加至建模器	可以在建模器板的供应文件夹中找到 Identity Manager 用户应用程序驱动程序。 
3	完成用户应用程序驱动程序配置	请参见 “完成用户应用程序驱动程序配置” 在第 71 页 中的过程。
4	访问供应视图	请参见 “访问供应视图” 在第 74 页 。
5	启动目录提取层编辑器	请参见 “要打开目录提取层编辑器，请执行以下操作：” 在第 75 页 。

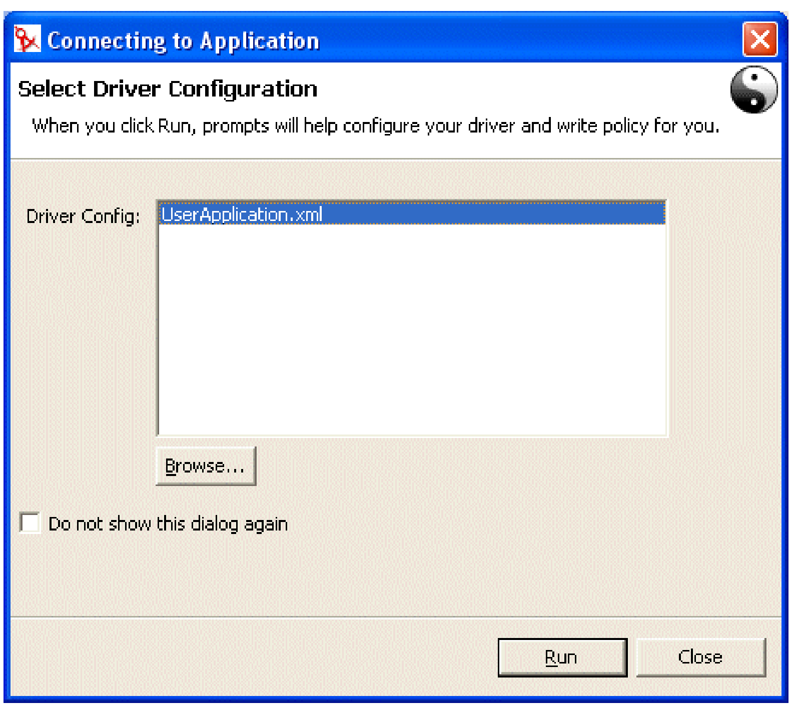
4.2.1 完成用户应用程序驱动程序配置

创建 Identity Manager 项目后，请按以下步骤操作。

要完成用户应用程序驱动程序配置，请执行以下操作：

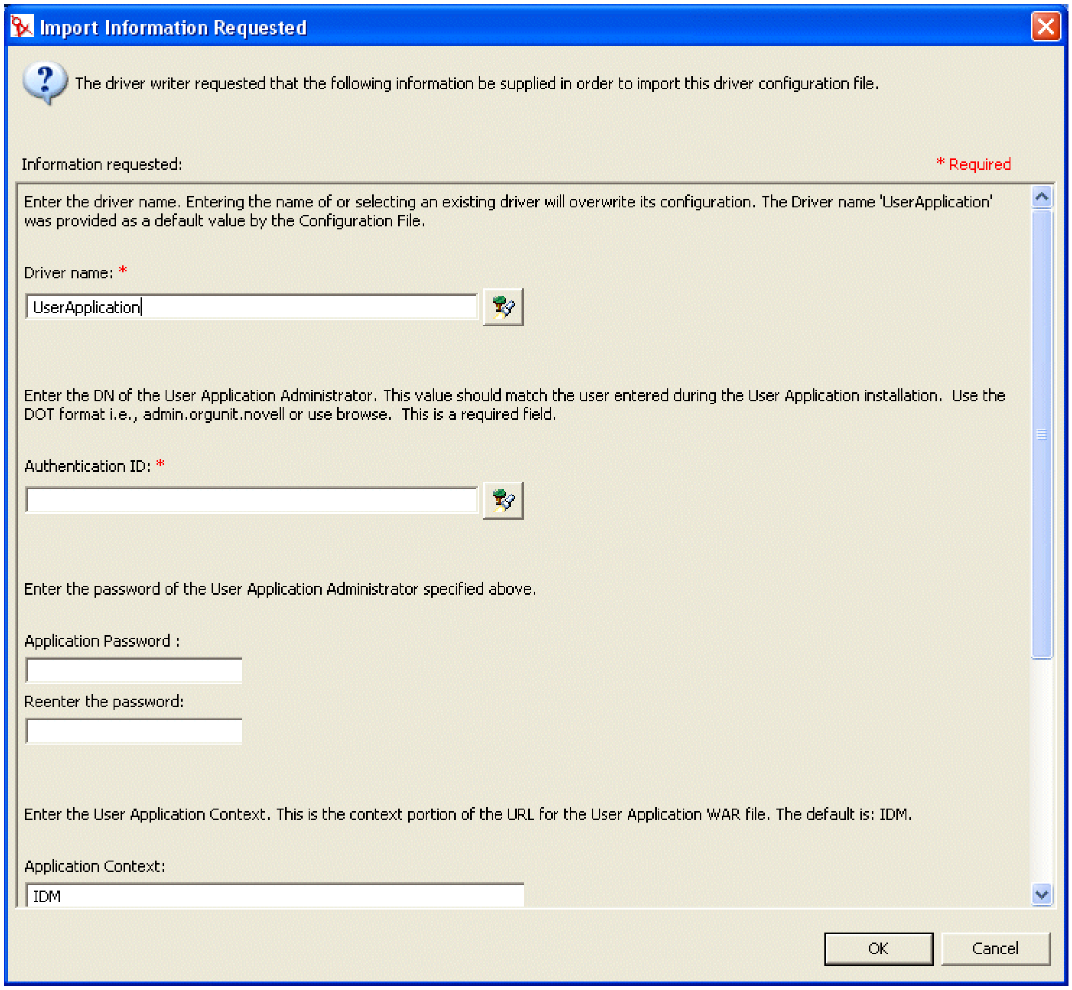
1 将 《用户应用程序》驱动程序图标拖放到画布上。

系统将提示进行驱动程序配置。



2 选择 *UserApplication.xml* （默认选项），然后单击 《运行》。

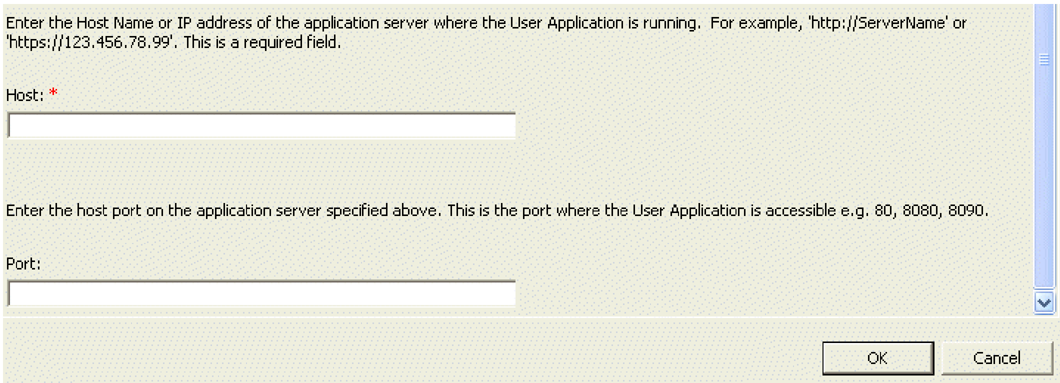
3 通过单击 《是》或 《否》指定向导应如何处理各项的验证。



.

.

.



4 根据如下介绍填写面板中的内容：

属性	指定的内容
驱动程序名	◆ 现有驱动程序的名称 （安装用户应用程序期间指定的驱动程序集中的驱动程序）。 ◆ 新驱动程序的名称。
鉴定 ID	用户应用程序管理员的 DN。
应用程序口令 / 再输入口令	用户应用程序管理员 （见上文）的口令。
应用程序环境	用户应用程序环境的名称 （安装时指定，如 IDM）
主机	部署 Identity Manager 用户应用程序的应用程序服务器的主机名或 IP 地址。此信息用于： ◆ 触发应用程序服务器上的工作流程以连接至访问工作流程 （终止、收回等）。 ◆ 更新超速缓存数据定义。
端口	见上文中 《主机》的端口。

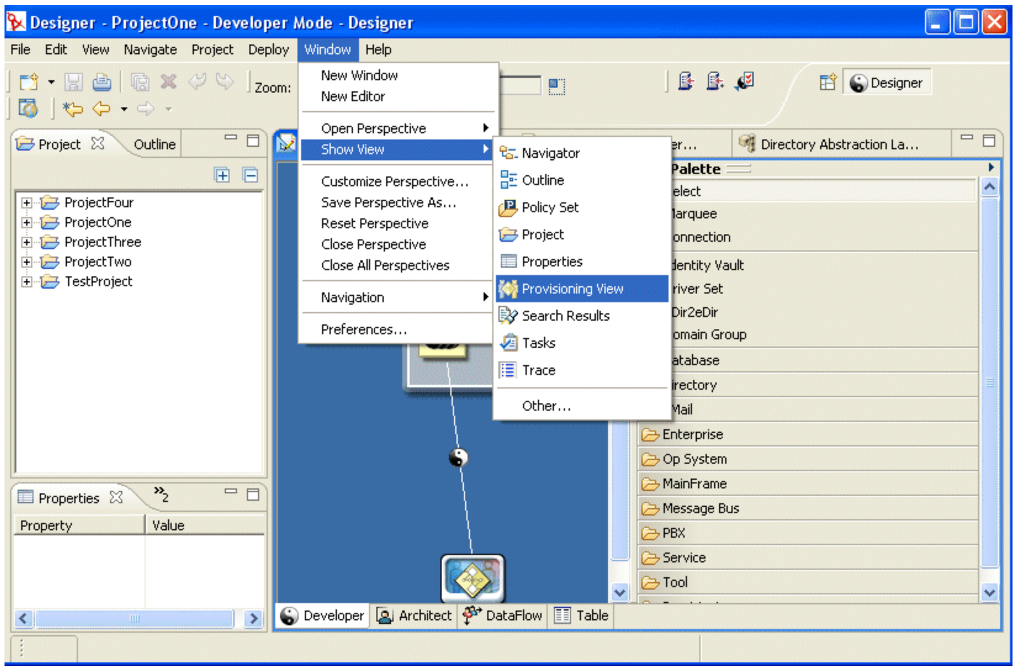
5 单击 《确定》。

4.2.2 访问供应视图

要访问供应视图，请执行以下操作：

1 请选择以下方法之一：

- 选择 《窗口》 > 《显示视图》 > 《供应视图》。



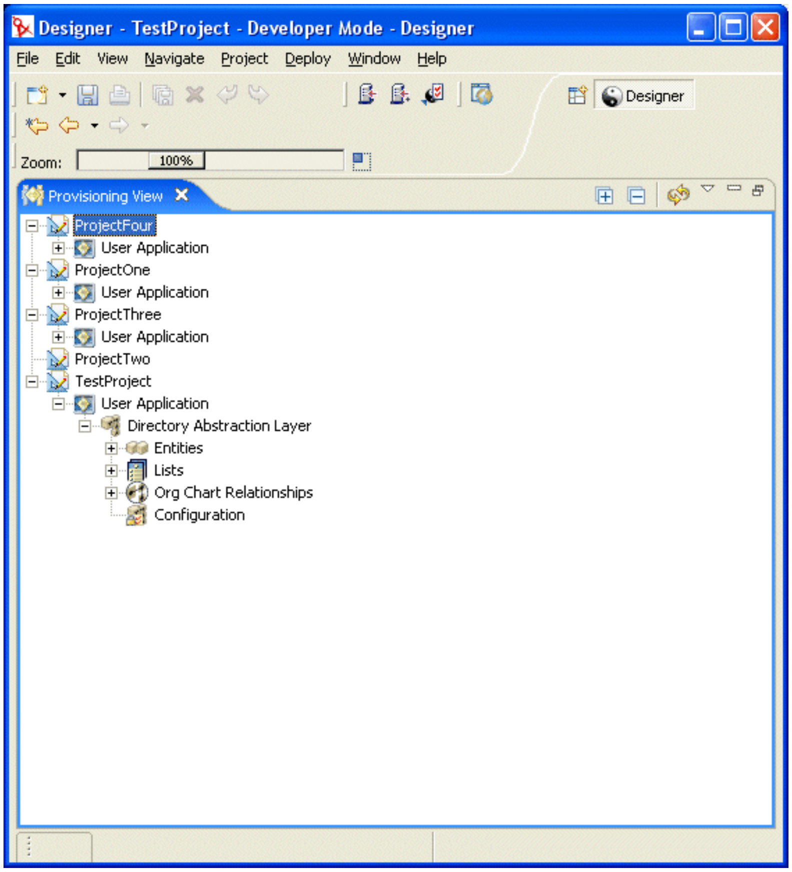
- 打开 《供应》 文件夹并选择 《供应视图》。
- 单击 《确定》。

或者

- 选择 《用户应用程序》 图标，单击鼠标右键并选择 《应用程序》 > 《显示供应视图》。

在供应视图中，可以看到刚创建的项目和位于同一工作空间的其它供应项目。

提示：如果在该视图中未看到所需的应用程序，可能是因为该项目已损坏。如果项目已损坏，则必须进行重创建。



关于供应视图

供应视图提供了对供应功能的永久访问权。在供应视图中双击某个项目将打开该项目的编辑器。使用供应视图可对目录提取层定义执行以下操作：

- 从 Identity Vault 中导入一个或多个对象定义。
- 验证数据定义的结构。
- 将定义部署到项目中指定的 Identity Vault 中。
- 创建和删除目录提取层定义。

有关更多信息，请参见 "导入、验证和部署目录提取层定义"在第 101 页 。

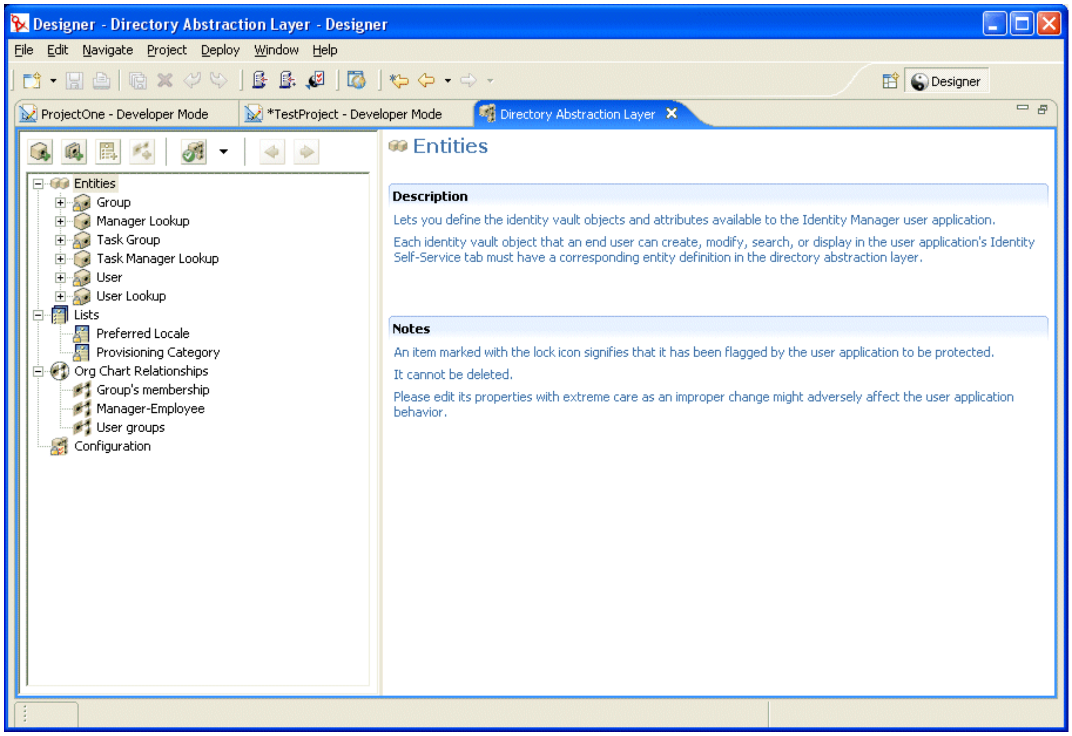
4.2.3 启动目录提取层编辑器

要打开目录提取层编辑器，请执行以下操作：

1 在 《供应视图》打开的情况下，导航至 《目录提取层》节点。

2 双击 《目录提取层》节点。

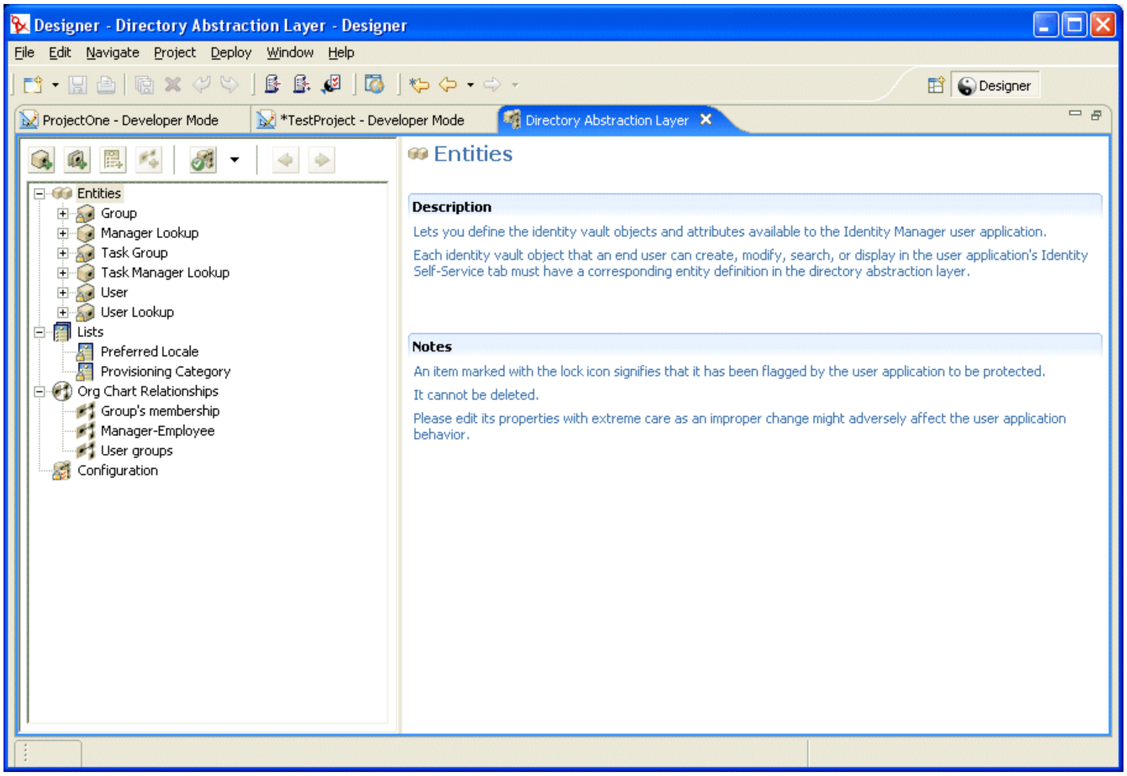
将出现一个树，其中包含 《实体》、《列表》、《组织结构图关系》和 《配置》。



关于目录提取层编辑器

目录提取层编辑器提供了定义包含目录提取层的 XML 文件集的图形方式。目录提取层编辑器是一种基于 Eclipse 的工具，可通过 Identity Manager 项目的 《供应视图》进行访问。

首次打开目录提取层编辑器时，可以看到提取层对象的基集，每次创建新的供应项目时都会自动创建这些对象：



目录提取层编辑器的节点包括：

要素	说明
Entities （实体）	实体表示为此项目配置的、并且可由用户应用程序使用的 Identity Vault 对象。有两种类型的实体： ◆ **映射自纲要的实体**。这些实体表示通过用户应用程序直接呈现给用户且存在于 Identity Vault 中的对象。用户通常可以创建、搜索和修改这些类型的对象的特性。 ◆ **表示 LDAP 关系的实体**。也称为 DNLookup。这些实体表示已编制索引的搜索，还可用于支持要显示的特殊类型的特性。DNLookup 实体提供了有关 LDAP 对象之间关系的信息。DNLookup 实体被： ◆ 组织结构图入口小程序使用以确定关系。 ◆ 搜索列表、创建和细节入口小程序使用以提供弹出选择列表和 DN 环境。 有关更多信息，请参见 “定义实体” 在第 80 页 。
Lists （列表）	用于定义全局列表的内容。全局列表： ◆ 和特性相关联。当特性显示在用户应用程序中时，它会显示为下拉列表。 ◆ 用于在 iManager 中显示供应请求配置插件使用的类别。 有关更多信息，请参见 “使用列表” 在第 94 页 。

要素	说明
Org Chart Relationships（组织结构图关系）	由用户应用程序的《身份自助服务》选项卡的组织结构图操作使用。用于在基于纲要的实体间映射分级关系。 有关更多信息，请参见“使用组织结构图关系”在第 97 页。
Configuration（配置）	一般配置参数。 有关更多信息，请参见“使用配置设置”在第 100 页。

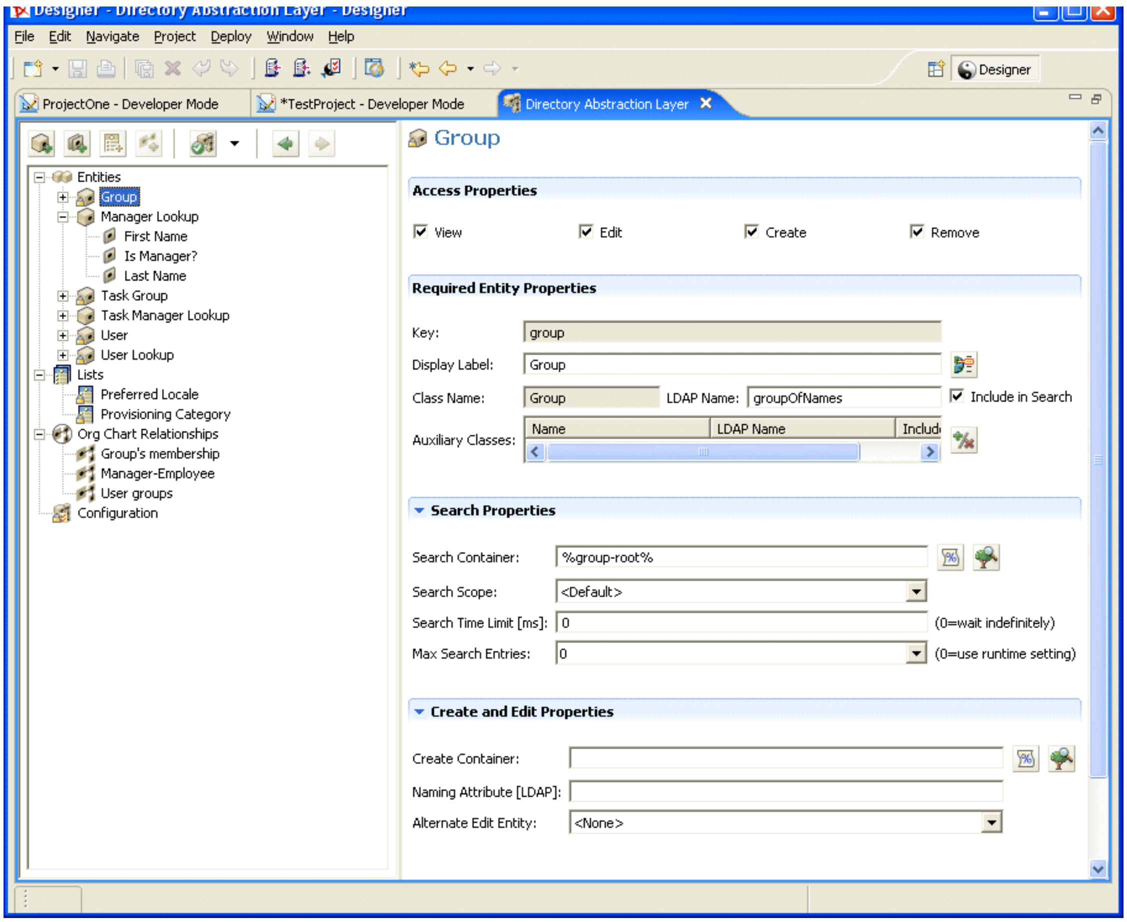
XML 文件本地储存的位置 目录提取层编辑器为每个实体、列表或关系均生成一个 XML 文件。这些文件储存在项目的 Provisioning\AppConfig\DirectoryModel 文件夹中。文件是根据对象的键命名的。其中包括：

目录	说明
ChoiceDefs	包含定义全局列表的文件。文件扩展名为 .choice。
EntityDefs	包含定义实体和特性的文件。文件扩展名为 .entity。
RelationshipDefs	包含定义组织结构图入口小程序可用的关系的文件。文件扩展名为 .relation。

可以使用目录提取层编辑器的功能来添加新定义，创建 Identity Vault 纲要模型。还可以使用供应视图的功能将新的定义部署到 Identity Vault。

使用目录提取层编辑器

目录提取层编辑器分为两个窗格。左窗格提供了目录提取层的内容视图。如果在左窗格中选择了一个项目，右窗格中将显示所选项目的特性和设置。



4.3 使用实体和特性

希望用户在 Identity Manager 用户应用程序中搜索、显示或编辑的任何 Identity Vault 对象都必须在目录提取层中定义为实体。例如，若要在用户应用程序中使用 Identity Vault 对象 inetOrgPerson，必须为该对象创建一个实体定义。

4.3.1 添加实体的步骤

请按照以下步骤将实体添加至目录提取层：

步骤	任务	详细信息
1	决定要在用户应用程序中使用的 Identity Vault 对象	“分析数据需求”在第 80 页
2	使用目录提取层编辑器定义目录提取层中的 Identity Vault 对象	“定义实体”在第 80 页
3	使用供应视图验证数据定义	“导入、验证和部署目录提取层定义”在第 101 页

步骤	任务	详细信息
4	将定义部署到 Identity Vault 中	"关于部署"在第 104 页
5	更新应用程序服务器的超速缓存，以包含新的提取层定义	第 13 章 "超速缓存配置"在第 199 页
6	测试 Identity Manager 用户应用程序，以确保正确显示所做的更改	

4.3.2 分析数据需求

要在目录提取层中创建 Identity Vault 数据模型，需要了解：

- 希望由 Identity Manager 用户应用程序使用的目录部分。

例如，用户可以搜索和显示的对象列表。对照提取层定义的基集检查此列表，以确定需要添加的内容。

- 包含自定义扩展和辅助类的纲要结构
- 包括以下内容的数据结构：
  - 必需的内容和可选的内容
  - 验证规则
  - 对象之间的关系 （DN 参照）
  - 特性的定义方式 （例如，表示电话号码的特性可能有多个值：家庭电话号码、办公电话号码和移动电话号码）
- 查看数据的人员

  这是一个公共站点还是私人站点？

拥有这些信息后，就可以使用它们将 Identity Vault 对象映射到提取层实体。

注释 : eDirectory ACL 适用于所有的提取层对象。对象和特性所具有的有效权限基于应用程序登录时所创建的已鉴定用户。

4.3.3 定义实体

根据在用户应用程序中想要显示的内容，可以定义以下两种实体：

- 映射自纲要的实体。这些实体表示在用户应用程序中直接呈现给用户且存在于 Identity Vault 中的对象。定义这种类型的实体时，将显示希望用户使用的所有特性。这种实体类型的示例包括：User （用户）、 Group （组）和 Task Group （任务组）。如果想要对不同类型的用户显示不同的特性集，还可以为同一个对象创建多个实体定义。有关更多信息，请参见 "为单个对象创建多个实体定义"在第 81 页 。
- 表示 *LDAP* 关系的实体。此类型的实体被称为 DNLookup，用户应用程序可以使用它进行以下操作：
  - 用相关实体间的 DN 搜索结果填充列表
  - 在更新和删除过程中保持 DN 参照特性之间的参照完整性

  组织结构图入口小程序使用支持 DNLookup 的实体来确定关系，并且搜索、创建和细节入口小程序还使用这些实体来提供弹出选择列表和 DN 环境。这种类型的实体示例包

括：Manager Lookup （管理员查找）、 Task Manager Lookup （任务管理员查找）和 User Lookup （用户查找）。有关更多信息，请参见“使用 DNLookup 控件类型”在第 91 页 。

为单个对象创建多个实体定义

可以创建多个实体定义，它们虽然表示同一 Identity Vault 对象，但提供不同的数据视图。在实体定义中可以：

- 为每个实体定义定义不同的特性

或者

- 定义相同的特性，但指定不同的访问属性以控制特性的搜索、查看、编辑或隐藏方式

注释 : 实体定义还可以包含可在结果集中隐藏某些实体的过滤器。

然后就可以在用户界面的不同部分使用这些不同的实体定义。例如，假定您希望创建员工目录；一个用于公共站点而另一个用于内部站点。在公共站点中，希望提供名和姓以及电话号码，而在内部站点中，则希望列出附加信息，如职务、经理等。以下是具体的创建步骤：

1. 创建两个实体定义 （具有不同的键）。

   两个实体定义都显示同一个 Identity Vault 对象，但是一个实体定义键为 public-staff-information，而另一个为 internal-staff-information。
2. 在每个实体定义中，定义不同的特性集：一个用于 public-staff-information，另一个用于 internal-staff-information。
3. 使用 Identity Manager 用户应用程序的 《入口小程序管理》选项卡为公共页和内部页分别创建一个入口小程序实例。

   有关创建入口小程序实例的更多信息，请参见第 9 章 “入口小程序管理”在第 165 页 。

创建实体定义的过程

确定了要显示的实体和特性后，就可以使用编辑器将它们添加到目录提取层中。请按照以下步骤进行操作：

步骤	操作	参见此过程
1.	决定从哪组文件开始。	
	◆ 想要添加至定义的基集	“添加实体的步骤”在第 79 页
	◆ 想要以已部署的定义开始	“关于导入”在第 101 页
1a.	希望使用的某些实体不是 eDirectory 基本纲要的一部分。eDirectory 纲要的任何扩展都不会自动显示在编辑器的可选对象和特性列表中。这意味着必须更新设计程序的本地纲要文件以包括这些自定义对象和特性。	“要更新可用纲要要素的列表，请执行以下操作：”在第 82 页
2.	将一个或多个实体添加到目录提取层中	“添加实体”在第 82 页
3.	将特性添加至实体	“添加特性”在第 84 页

更新可用纲要要素的列表

要更新可用纲要要素的列表，请执行以下操作：

1 打开 Identity Manager 项目，选择 Identity Vault，单击鼠标右键并选择 *Live Operations > Import Schema* （实时操作 > 导入纲要）。
2 选择 *Import from eDirectory* （从 eDirectory 导入）并提供 eDirectory 主机规格。
3 单击 《下一步》。
4 选择要导入的类和特性，然后单击 《完成》。

添加实体

可以通过 《添加实体向导》（下文中介绍）或单击编辑器工具栏中的 《添加实体》按钮来添加实体。

注释：使用 《添加实体》按钮时，系统将提示选择所创建实体的对象类。编辑器会自动将必需特性添加到实体中。然后可以使用 《添加特性》对话框完成实体定义。

要使用 《添加实体向导》添加实体，请执行以下操作：

1 以下列方法之一起动 《添加实体向导》：

   从 *Provisioning View* （供应视图）中：

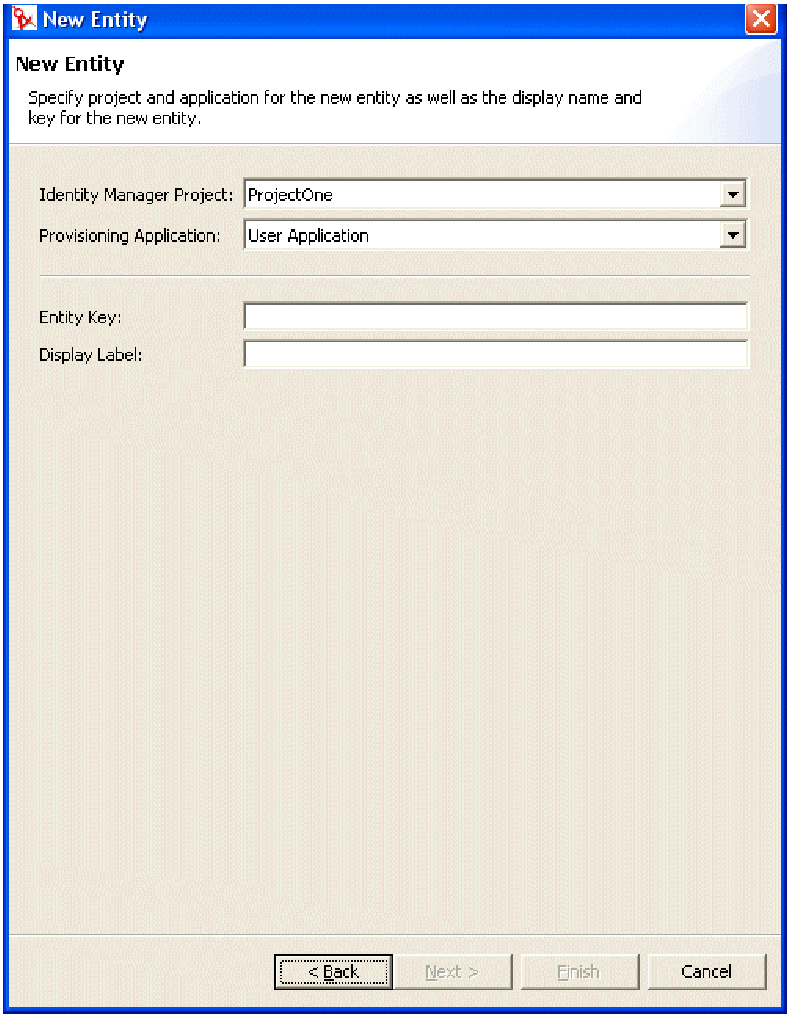
   - 选择 《实体》节点，单击鼠标右键，然后选择 《新建》。
   - 选择 《文件》 > 《新建》 > 《供应》。选择 《目录提取层实体》。单击 《下一步》。

   从目录提取层编辑器中：

   - 选择 《实体》节点，单击鼠标右键，然后选择 *New Entity-Attributes Wizard* （新建实体 - 特性向导）。

     即显示 《新建实体》对话框。

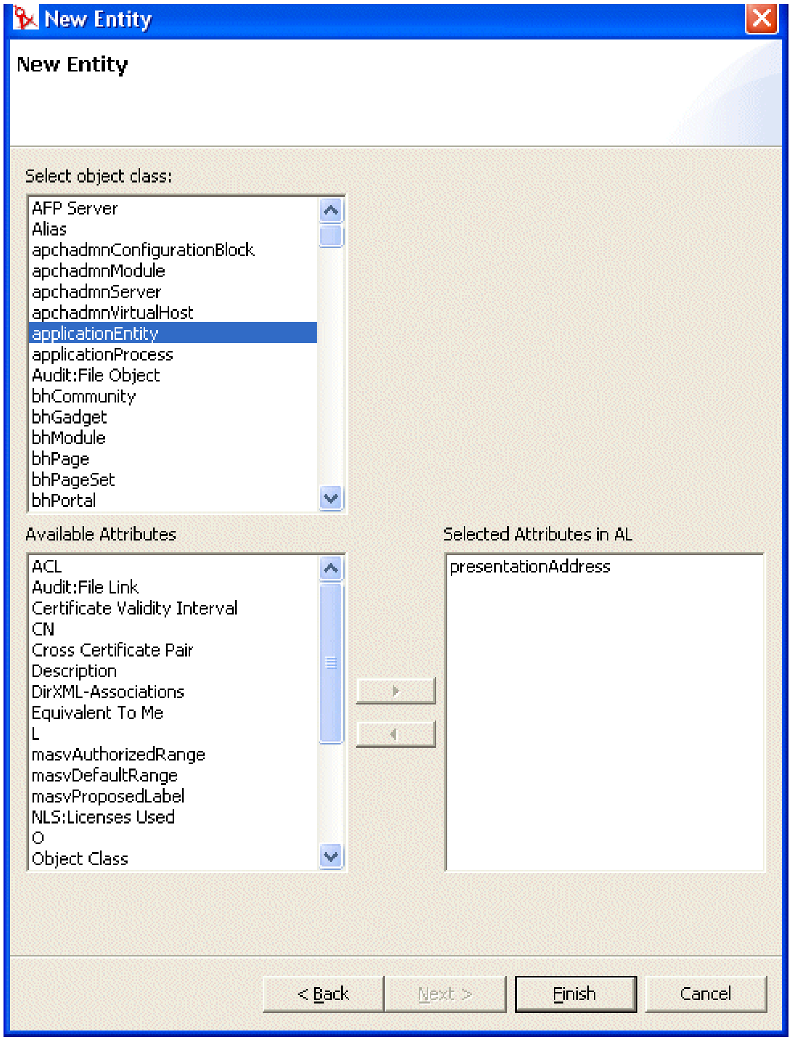
   注释：如果从 《文件》菜单中起动，对话框中将包含使用以上两种方法起动时不会显示的字段。如下图所示。



2 根据如下介绍填写面板中的内容：

字段	说明
《Identity Manager 项目》和 《供应应用程序》	选择要添加实体和特性的 Identity Manager 项目和供应应用程序。 **注释：**从 《文件》菜单起动向导时会显示这些字段。
实体键	实体的唯一标识符。
显示标签	在用户界面中引用该实体时，就会显示该字符串。

3 单击 《下一步》。即显示 《新建实体》对话框：



4 选择要创建的实体的对象类，然后从 《可用特性》列表中选择所需的特性

提示：如果要创建的实体的对象类没有显示在 Available Object Classes （可用对象类）列表中，则可能需要更新设计程序的本地纲要文件。请按照 “要更新可用纲要要素的列表，请执行以下操作：” 在第 82 页 中的步骤进行更新。

---

5 单击 《完成》。

即显示属性页以供编辑。

有关更多信息，请参见 “实体的属性参照” 在第 86 页 。

注释：要将特性提供给用户应用程序使用，必须部署包含该特性的实体。

添加特性

要添加特性，请执行以下操作：

1 选择一个实体。

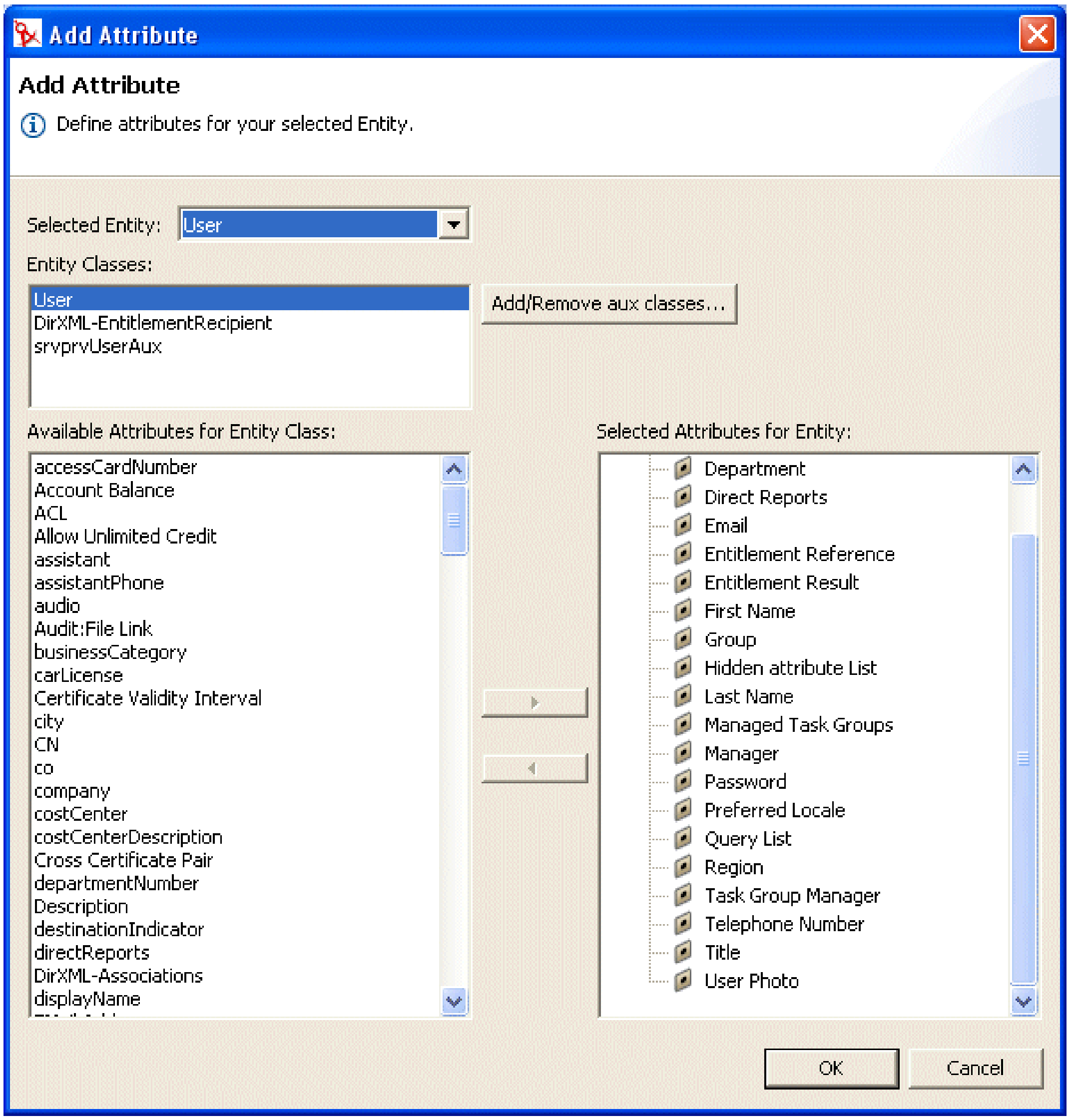
2 通过以下方法添加特性：

- 右键单击并选择 《添加特性》。

或者

- 单击 《添加特性》图标。

将弹出下面的提示对话框：



3 从 *Available Attributes for Entity Class* （实体类的可用特性）列表中选择特性，然后将它添加到 *Selected Attributes for Entity* （实体的所选特性）列表中。

提示：如果要创建的特性没有显示在 《实体类的可用特性》列表中，则可能需要更新设计程序的本地纲要文件。请按照 "要更新可用纲要要素的列表，请执行以下操作：" 在第 82 页 中的步骤进行更新。

---

4 单击 《确定》。

即显示属性页以供编辑。

有关更多信息，请参见 “特性的属性参照”在第 88 页 。

注释 : 要使特性可用于用户应用程序，必须进行部署。

实体的属性参照

可以对实体设置以下类型的属性：

- “实体的访问属性”在第 86 页
- “实体的必需属性”在第 86 页
- “实体的搜索属性”在第 87 页
- “实体的创建和编辑属性”在第 87 页
- “口令管理属性”在第 88 页

实体的访问属性

访问属性 控制用户应用程序如何与实体进行交互。其中包括：

属性	说明
创建	选中 - 用户应用程序可以创建此对象。
编辑	取消选中 - 不管基础 ACL 如何，用户应用程序都无法更改此对象。
	选中 - 可能能够更改此对象，但由 Identity Vault ACL 确定能否更改。
查看	选中 - 用户应用程序可以显示此对象。
去除	选中 - 用户应用程序可以删除此对象。

实体的必需属性

必需的实体属性包括：

属性名	说明
键	该实体的唯一标识符。它定义了用户应用程序参照此对象的方法。
显示标签	定义用户界面中对象的显示方式。
类名	Novell Directory Service (NDS) 类名。
LDAP 名称	LDAP 对象类名称。
搜索	选中 - 可以搜索此实体。必须选中身份入口小程序 （如实体搜索列表或实体组织结构图）在查询中使用的实体 (True)。
辅助类	此实体的辅助类列表，该列表中可以没有辅助类，也可以有多个辅助类。
	如果添加辅助类，必须指定辅助类的 LDAP 名称、 NDS 名称以及该辅助类是否可以被搜索。

实体的搜索属性

实体的搜索属性包括：

属性名	**说明**
搜索树枝	搜索开始处的 LDAP 节点或树枝 （搜索根）的判别名。例如： `ou=sample,o=ourOrg` 可以浏览 Identity Vault 来选择树枝，也可以使用 “使用预定义的参数” 在第 88 页 中说明的某个预定义参数。
搜索范围	指定相对于搜索根而言，在什么范围内搜索。 值为： **< 默认 >** - 此搜索范围与选择树枝和从属树枝时的范围一样。 **树枝** - 在搜索根 DN 和搜索根级别的所有项中进行搜索。 **树枝和从属树枝** - 在搜索根 DN 和所有从属树枝中进行搜索。与选择 **< 默认 >** 时的搜索范围相同。 **对象** - 将搜索范围限定在指定的对象中。此搜索用于验证指定的对象是否存在。
搜索时间限制 [ms]	以毫秒为单位指定一个值，或将值指定为 0 以表示没有时间限制。
最大搜索项	指定希望搜索返回的搜索结果项的最大数目。 如果要使用运行时设置，请将其指定为 0。 建议： 为达到最高效率，请将值设定在 **100 到 200** 之间。 **不要**设定超过 1000 的值

实体的创建和编辑属性

实体的创建和编辑属性包括：

属性名	**定义**
创建树枝	创建此类型新实体的树枝的名称。 可以浏览 Identity Vault 来选择树枝，也可以使用 “使用预定义的参数” 在第 88 页 中说明的某个预定义参数。 如果没有指定此值，则创建入口小程序将提示用户为新对象指定树枝。该入口小程序将使用实体定义中指定的搜索根作为基址，并允许用户从此处向下钻取。如果实体定义中没有指定搜索根，将使用用户应用程序安装期间指定的根 DN。
命名特性	实体的命名特性 （相对判别名 (RDN)）。对于选择了 《创建》访问参数的实体，此值才是必需的。

属性名	定义
替换编辑实体	编辑实体的特性显示在细节入口小程序的编辑模式下。 从下拉列表中选择实体，如果细节入口小程序没有显示此实体，请选择 <None>。

口令管理属性

口令管理属性包括：

属性名	定义
口令特性	选择将储存此实体口令的特性。
创建特性时的必需口令	**选中** - 表示在创建此实体时需要口令。

使用预定义的参数

可通过目录提取层编辑器对某些值使用预定义的参数。这些参数是：

预定义的参数	说明
%driver-root%	表示供应驱动程序 DN。在安装过程中进行用户应用程序配置时，或稍后进行配置时指定此值。它储存在用户应用程序域配置中。
%user-root%	表示用户树枝 DN。在安装过程中进行用户应用程序配置时，或稍后进行配置时指定此值。它储存在用户应用程序域配置中。
%group-root%	表示组树枝 DN。在安装过程中进行用户应用程序配置时，或稍后进行配置时指定此值。它储存在用户应用程序域配置中。

特性的属性参照

可以设置特性的以下属性：

- "特性的访问属性" 在第 88 页
- "特性的必需属性" 在第 89 页
- "特性的过滤器和格式属性" 在第 89 页
- "特性的 UI 控件属性" 在第 90 页

特性的访问属性

特性的访问属性包括：

名称	说明
编辑	**选中** - 可以通过用户应用程序编辑 / 修改此特性。即使已将此特性选中 (True)，但如果基本 Identity Vault ACL/ 有效权限禁止它，此特性可能仍无法编辑。
启用	**取消选中** - 用户应用程序无法使用此特性。与从文件中去除项效果相同。

名称	说明
隐藏	控制启用或禁用用户应用程序中的 《隐藏》复选框。用户可以使用 《隐藏》复选框控制应用程序是否显示某特性 （如用户的照片）。 **取消选中** - 此特性的 《隐藏》复选框被禁用，用户将无法选择隐藏此特性。 **选中** - 可以在用户应用程序中启用 《隐藏》复选框。但登录用户还必须符合以下条件。他们： ◆ 为该特性的拥有者，或者为用户应用程序管理员。 ◆ 具有受托者权限，可以更新 Identity Vault 中的 srvprvHideAttributes 特性。 如果不符合这些要求，即使选中此设置 (True)，用户界面的 《隐藏》复选框仍将被禁用。 **提示 :** 如果某用户隐藏了包含图像的特性，则正在查看此图像的用户仍可能继续看到此特性，直到该用户的浏览器超速缓存被刷新。
多值	指定是此特性是否可以有多个值，如电话号码。 **选中** - 此特性可以有多个值。
读	**选中** - 用户应用程序可以查询此特性。大多数特性都会选择此属性 (True)，但对某些特性 （如口令）则需取消选中此属性。
必需	**选中** - 必须提供此特性。
搜索	**选中** - 用户应用程序可以搜索此特性。必须选中身份入口小程序 （例如，实体搜索列表或实体组织结构图）在查询中使用的特性。 **提示 :** 如果已在 eDirectory 中对搜索时使用的特性编制索引，搜索速度会更快。
查看	**选中** - 用户应用程序可以显示此特性。大多数情况下都可选中此属性，但对于某些特性 （如口令）可能要取消选中此属性。

特性的必需属性

名称	说明
键	特性的唯一标识符。
显示标签	在用户应用程序中显示的标签。
特性名称	特性的 NDS 名称。
LDAP 名称	特性的 LDAP 名称。

特性的过滤器和格式属性

名称	说明
过滤器：WHERE 特性	可以指定在 Identity Vault 中搜索此特性的 LDAP 过滤器。
启用	**选中** - 启用此过滤器。

特性的 UI 控件属性

名称	说明
数据类型	从以下列表中选择数据类型： ◆ 二进制 ◆ 布尔值 ◆ DN ◆ 整数 ◆ 本地化字符串 ◆ 字符串 ◆ 时间
格式类型	用户应用程序使用它设置数据的格式。格式类型包括： ◆ 无 ◆ AOL IM ◆ 电子邮件 ◆ Groupwise IM ◆ 图像 ◆ 电话号码 ◆ Yahoo IM ◆ 图像 URL ◆ 日期 ◆ 日期时间 格式类型取决于数据类型。例如，时间数据类型只能与日期格式及日期时间格式相关联。

<table>
<tr><th>名称</th><th>说明</th></tr>
<tr><td>控件类型</td><td>
控件类型包括：

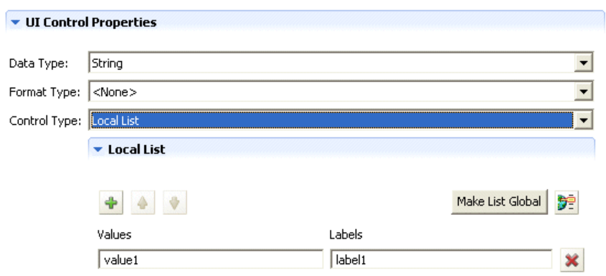
DNLookup - 定义此特性中包含 DN 参照。适用于以下情况：
◆ 用相关实体间的 DN 搜索结果填充列表
◆ 在更新和删除过程中保持 DN 参照特性之间的参照完整性

用户应用程序使用此信息生成特殊的用户界面要素，并根据 DNLookup 定义执行优化搜索。

有关更多信息，请参见 “使用 DNLookup 控件类型” 在第 91 页 。

全局列表 - 将此特性显示为下拉列表，列表中的内容在此特性定义以外的文件中定义。

有关更多信息，请参见 “使用列表” 在第 94 页 。

本地列表 - 将此特性显示为下拉列表，列表的内容与此特性一起定义。要定义本地列表，请执行以下操作：
1. 选中此特性后，将控件类型设置为 Local List （本地列表）。


2. 单击 《添加》按钮可添加更多值。使用上下箭头按钮可更改项目在列表中的位置。
在 《值》列中，键入需写入 Identity Vault 的值。其中只能包括小写字母、数字和下划线 (_) 字符。
3. 在 《标签》列中，键入显示在用户界面中的文本。

范围 - 使用 《范围》控件类型和 《整数》数据类型，可将用户输入范围限制为连续值。需要提供范围的起始和终止值。
</td></tr>
</table>

使用 **DNLookup** 控件类型

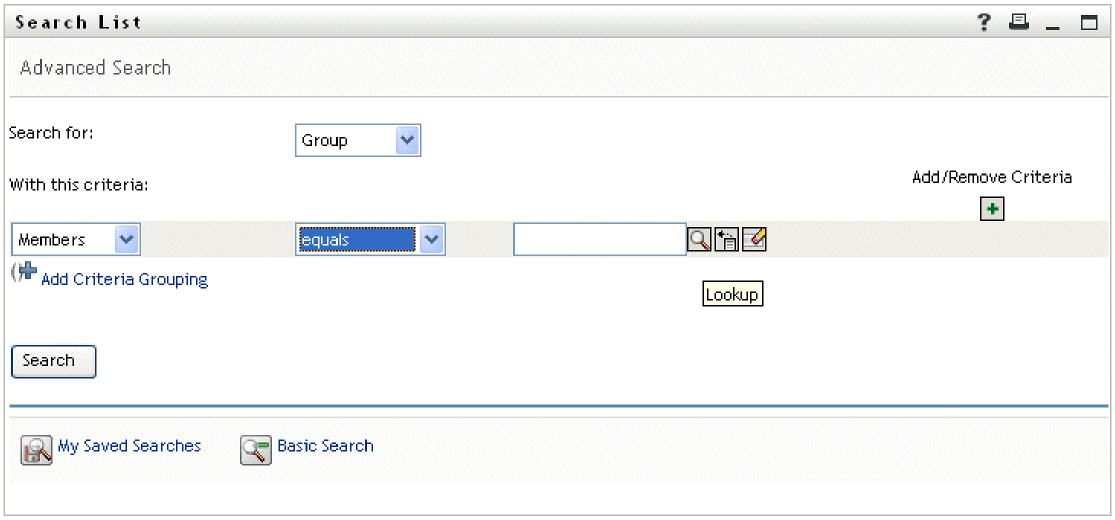
如果将控件类型定义为 DNLookup，则意味着：

- 搜索此特性时，用户可从可能的值列表中进行选择。
- 创建、填充或删除此特性时，将根据用户操作 （创建、删除、更新）相应地更新相关实体中的特性，以维持参照完整性。

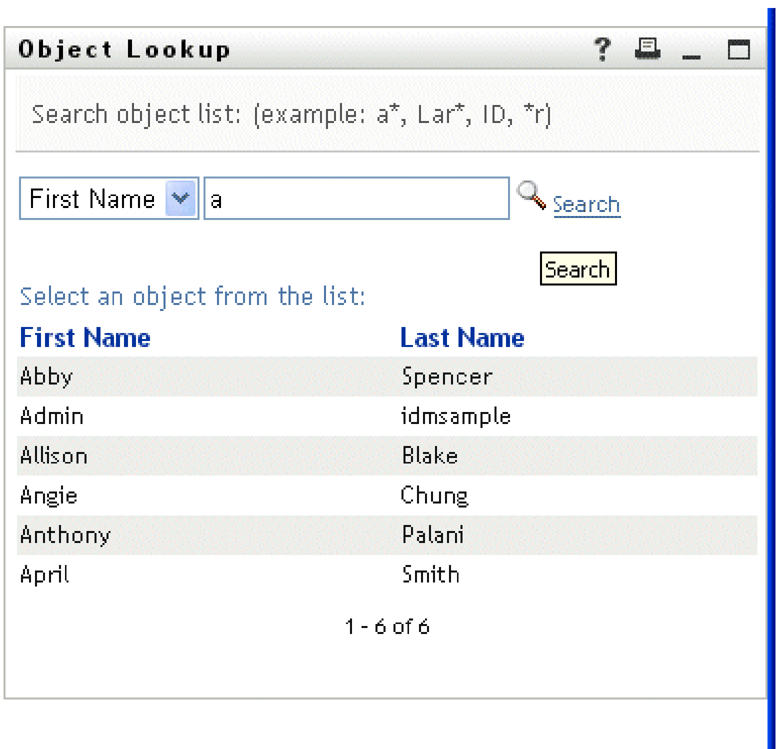
用于选择列表的 DNLookup

已安装的用户应用程序中包含用户实体定义和组实体定义。用户实体定义中又包含名为 Group 的特性，该特性被定义为 DNLookup 控件类型。这样身份入口小程序就可以为特定用

户提供组选择列表。例如，某用户要进行目录搜索。他想要查找组中的用户，但不知道组名。他可以选择 《用户》作为搜索对象，并将 《组》设为搜索准则，如图所示：



由于已将 《组》定义为用户实体的 DNLookup 控件类型，因此将显示 《查找》图标。如果用户选择此图标，则显示可能的组列表：



用户可从列表中选择某个组。

用于参照完整性的 DNLookup

由于 LDAP 允许组关系在两个方向映射，因此用于更新和同步的 DNLookup 非常重要。例如，可以将数据设置为：

- 用户对象中包含 group 特性。该 group 特性：
- 为多值
- 列出用户所属的所有组
- 组对象中包含 user 特性。该 user 特性：
- 为多值
- 列出属于该组的所有用户

这意味着，在用户对象中可以有一个特性，显示该用户所属的所有组；在组对象中可以有一个 DN 特性，包括该组中的所有成员。

用户请求更新时，用户应用程序必须认可此关系，并确保目标特性和源特性同步。可以在 DNLookup 中指定这两个特性必须同步。用这种方法可以在任何相关对象之间 （不仅是组结构对象）进行同步。根据 *DNLookup* 关系完整性属性参照中描述的方法指定 DNLookup 高级属性，可以创建此类 DNLookup 控件类型。

DNLookup 属性参照

DNLookup 显示属性包括：

字段	定义
查找实体	要搜索的实体名称，例如，任务组实体中包含任务管理员特性。要填充此字段，需要知道哪些用户是任务管理员。
细节实体	用户单击用户应用程序中的超文本链接以请求更多信息时，所显示的细节所属的实体键。如果定义了 DNLookup，身份入口小程序就可以提供超文本链接，允许用户查看被链接对象的细节。
要显示的特性	选择在搜索完成后要显示的一个或多个特性。
执行自动查询	定义**要显示的特性** （见上）如何显示。 ◆ **选中** - 执行实体的自动查询，并在可选列表中显示结果。如果返回的数据很多，用户可能不希望选择此选项，因为用户必须在一个大的结果集中滚动。 ◆ **取消选中** - 允许用户指定实体查询的搜索准则，然后在可选列表中显示结果。

DNLookup 关系完整性属性 - 这些属性用于同步两个对象 （例如，组和组成员）之间的数据。

属性	定义
要更新的源特性	要更新的特性名称。此特性中必须包含**要更新的目标特性**的 DN 参照。要同步两个不同对象的特性，需要此属性。

属性	定义
要更新的目标特性	必须与**要更新的源特性**同时更新的特性名称。这是一个 LDAP 特性名称。要同步两个不同对象的特性，需要此属性。此特性必须包含一个 DN 参照。
目标辅助类 （可能有）	包含**要更新的目标特性**的辅助类名称。

4.4 使用列表

可以使用列表节点定义全局列表的内容。Identity Manager 用户应用程序使用全局列表以：

- 提供特性的值列表。在用户界面中显示此特性以进行编辑时，可能的值显示在下拉列表中。
- 用于定义 iManager 的供应请求配置插件的可用类别。这是一个专用列表。有关详情，请参见 “关于供应类别列表”在第 96 页 。

要新建全局列表，请执行以下操作：

1 通过以下任一方式起动 《新列表向导》：

从 《供应视图》中：

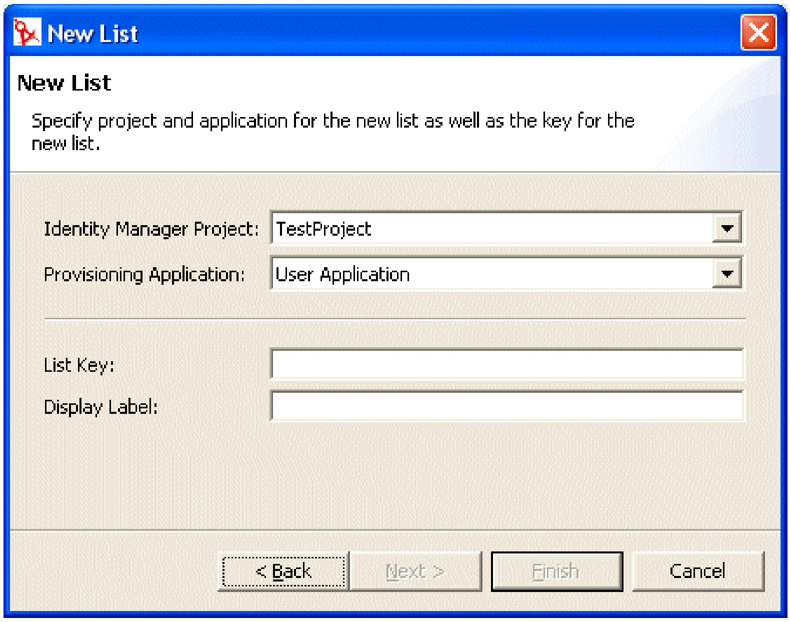
- 选择 《文件》 > 《新建》 > 《供应》。选择 *Directory Abstraction Layer List* （目录提取层列表）。单击 《下一步》。
- 选择 《列表》节点，单击右键并选择 《新建》。

从目录提取层编辑器 中：

- 单击 *New List* （新建列表）按钮。
- 选择 《列表》节点，单击右键并选择 *Add List* （添加列表）。

显示 《新建列表》对话框。

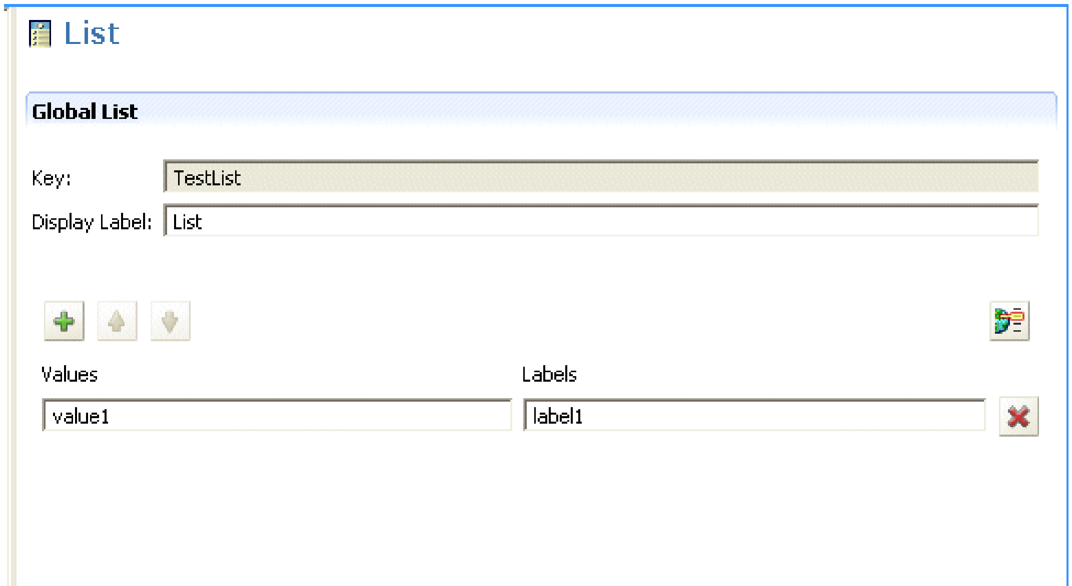
注释 : 如果从 《文件》菜单中起动，对话框中将包含使用以上两种方法起动时不会显示的字段。



2 根据如下介绍填写面板中的内容：

字段	说明
《Identity Manager 项目》和 《供应应用程序》	选择要添加实体和特性的 Identity Manager 项目和供应应用程序。 **注释：**从 《文件》菜单起动向导时会显示这些字段。
列表键	列表的唯一标识符。
显示标签	在用户界面中参照此列表时使用的字符串。

3 单击 《完成》。将显示 《全局列表》属性页。



4 请填写这些字段：

字段	说明
显示标签	在设计程序中显示的列表名称。
标签	用户界面中显示的列表项文本。
值	要储存在 Identity Vault 中的列表项的值。其中只能包括小写字母、数字和下划线 (_) 字符。

现在即可在设计环境中使用此列表。

5 保存此项目。

注释：要在运行时环境中使用此列表，必须进行部署。

4.4.1 关于优先的区域设置列表

在浏览器语言不是所支持语言的情况下，优先的区域设置列表表示要使用的默认语言。所显示的列表内容是用户应用程序中编辑用户操作的默认配置。

4.4.2 关于供应类别列表

供应类别列表定义的类别集有助于组织受供资源 （权利）和供应请求。此列表中的类别显示在：

- *iManager* - 供应请求配置插件
- 用户应用程序 - 《请求和批准》选项卡

不能更改供应请求列表键，但可以向列表中添加更多项或更改现有类别的值和标签。

要修改供应类别列表的内容，请执行以下操作：

1. 请确保在编辑器中打开正确的项目。
2. 单击 《列表》节点。
3. 选择 《供应类别》。
4. 使用全局列表属性窗格进行修改。

注释 **:** 请在 《值》字段中填充类别键。在类别键中，只有小写字母、数字和下划线 (_) 字符是有效字符，因此 《值》字段仅限于这些字符。类别键在内部用作类别标识符。

---

5. 保存并部署所做的更改。切记更新应用程序服务器的超速缓存。

   部署更改后，这些更改就会反映在用户应用程序和 iManager 插件中。

4.5 使用组织结构图关系

可以使用 《组织结构图关系》节点定义实体间的分级关系，这些实体是在目录提取层中定义的。这种关系可以在类似实体 （例如，用户 / 用户）或不同实体 （例如，用户 / 设备）间定义。

以下是为用户应用程序定义的关系：

- 组成员资格
- 经理 - 员工
- 用户组

要成功部署关系，必须首先部署该关系的所有部件 （实体和特性）。

要新建关系，请执行以下操作：

1. 可以使用以下任一方式新建关系：

   从 《供应视图》中：

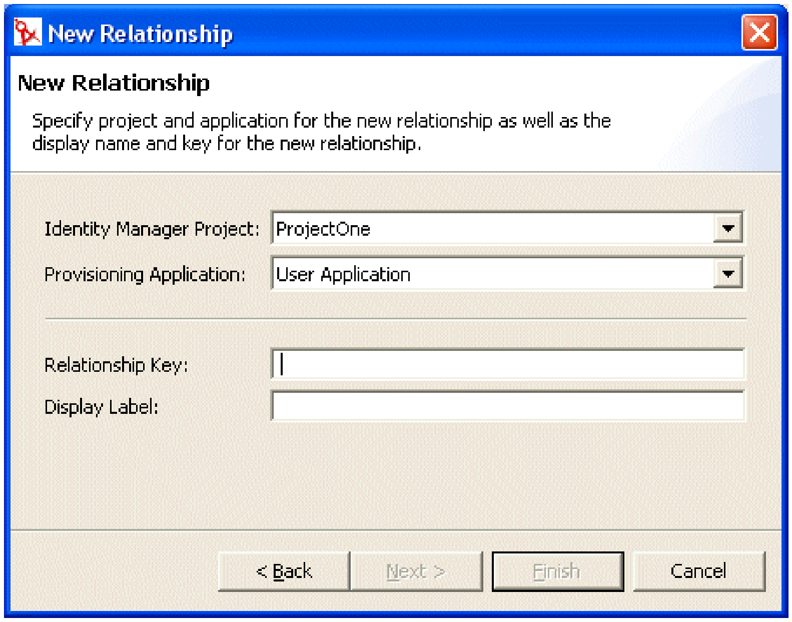
   - 选择 《文件》 > 《新建》 > 《供应》。选择 *Directory Abstraction Layer Relationship* （目录提取层关系）并单击 《下一步》。
   - 选择 *Org Chart Relationships* （组织结构图关系）节点，单击右键，然后选择 《添加》。

   从目录提取层编辑器中：

   - 单击 *Add Relationship* （添加关系）按钮。
   - 选择 《组织结构图关系》节点，单击右键，然后选择 《添加关系》。

   显示 《新建关系》对话框。

注释 **:** 如果从 《文件》菜单中起动，对话框中将包含使用以上两种方法起动都不显示的字段。

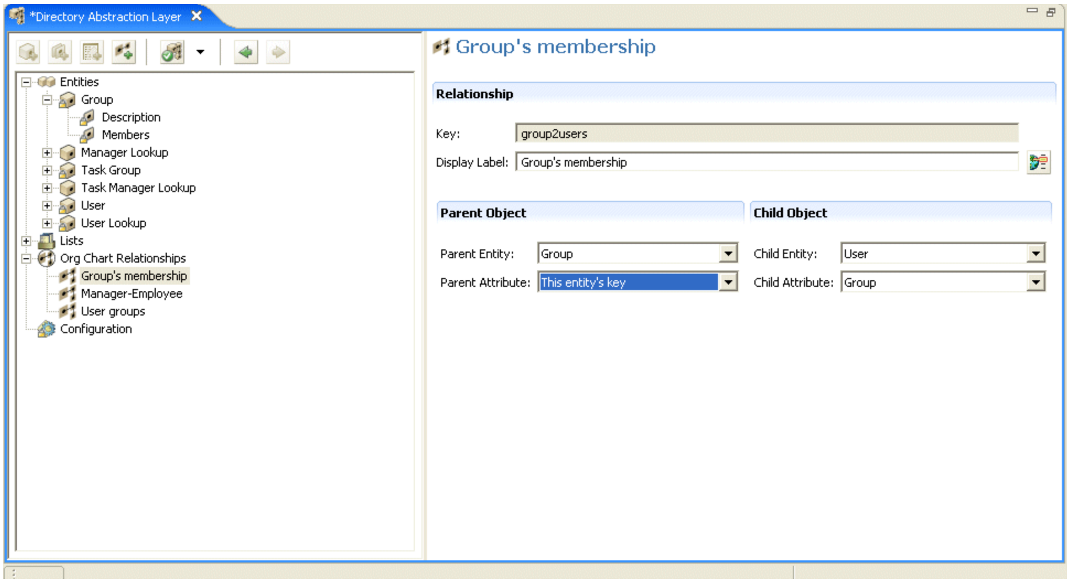


2 根据如下介绍填写面板中的内容：

字段	操作
《Identity Manager 项目》和 《供应应用程序》	请确保已选中正确的 Identity Manager 项目和供应应用程序。
	注释 **:** 如果从 《文件》菜单中创建关系，将显示此字段。
关联关键字	键入关联关键字的唯一值。
显示标签	键入关系出现在 Identity Manager 用户界面中时所显示的字符串。

3 单击 《完成》。

关系已创建，其属性页也会打开，可进行编辑。



4.5.1 关系的属性参照

字段	说明
键	关系唯一的只读标识符。 提示：在组织结构图入口小程序自选设置页中指定此值。
显示标签	指定其它身份入口小程序参照此关系时显示的名称。例如，用户在细节入口小程序中单击 《选择组织结构图》图标时显示此值。 单击 《本地化》，提供显示标签文本的转换。
父实体	从下拉列表中选择一个实体。 所选的实体将成为组织结构图层次中的父对象。例如，在经理 - 员工关系中，父实体为用户。在组 - 成员关系中，父实体为组。 **目录提取层要求** - 此列表中的实体为目录提取层中所定义实体的子集。必须选中父实体的视图访问属性 (True)
父特性	从下拉列表中选择一个特性。 将使用此特性查找匹配的子实体。如果此特性的值和子实体特性的相应值匹配 （请参见下面的 《子特性》），即可建立关系。 **目录提取层要求** - 将使用所选父实体的特性填充此特性列表。其中仅包括定义为 DNLookup 控件类型的特性
子实体	选择将作为层次中子对象的实体。例如，在经理 - 员工关系中子实体为用户。在员工 - 资源关系中子实体为设备。 此实体中必须包含与父特性相关的特性。

字段	说明
子特性	选择与父特性匹配的特性。 可以指定用于查找匹配的父实体的子实体特性。如果此特性的值与父实体特性的相应值匹配 （请参见上述 《父特性》），即可建立关系。

注释 **:** 组织结构图入口小程序不完全支持动态组。不能将动态组定义为关系中的父实体，但可以将动态组定义为关系中的子实体。

要删除关系，请执行以下操作：

1 选择要删除的关系。
2 单击右键并选择 《删除》。

4.6 使用配置设置

可以使用 《配置》节点设置用户应用程序的一般配置属性。其中包括：

属性	说明
默认的 ' 我的简报 ' 实体	定义用户在用户界面中单击 《我的简报》时所显示的实体。 此字段仅限于显示其对象类为用户 （或 LDAP inetOrgPerson）的实体。
默认的区域设置	定义在用户应用程序中显示标签时使用的默认语言。如果将浏览器设置为不支持的语言，则改为使用此区域设置。 注释 **:** 浏览器区域设置将覆盖所支持语言的默认区域设置。
树枝类	为创建用户操作或组操作提供树枝类的选择列表的内容。用户从选择列表中选择树枝，作为新建对象所驻留的位置。

4.7 本地化显示文本

目录提取层编辑器提供了一种简单的方法，可用于本地化以下内容的显示文本：

- 实体和特性显示标签
- 组织结构图关系名
- 全局列表项和本地列表项

4.7.1 支持的语言

可以对以下一种或多种语言的显示文本进行本地化：

- 英语
- 法语
- 德语
- 意大利语

- 日语
- 朝鲜语
- 葡萄牙语
- 俄语
- 简体中文
- 西班牙语
- 繁体中文

4.7.2 本地化文本

目录提取层编辑器提供了多种不同方法，来本地化提取层定义。可以通过以下方式访问本地化对话框：

要定义以下内容的本地化文本	操作
目录提取层中所有可进行本地化的项目	◆ 单击 **Set Global Localization** （设置为全局本地化）（在目录提取层编辑器工具栏中）。 请确保在目标字段中输入本地化文本前选择目标语言。
特定的实体、关系或列表	◆ 在目录提取层编辑器树视图中，选择要本地化的对象。 ◆ 单击右键并选择 《本地化》。 请确保在目标字段中输入本地化文本前选择目标语言。
一个显示标签	◆ 选择特定的实体或特性。 ◆ 单击 **Localize Display Label** （本地化显示标签）（该标签位于 《属性》窗格中 《显示标签》字段旁）。

这些对话框外观可能不尽相同，但都包含以下字段：

- 原始 - 通常为对象类型 （例如，实体、列表或关系）和键
- 源 - 要转换的文本 （显示标签）
- 目标语言 - 所支持的语言之一
- 目标 - 转换文本

4.8 导入、验证和部署目录提取层定义

导入、验证和部署目录提取层定义是在设计程序的 《供应视图》中执行的操作。

- “关于导入”在第 101 页
- “关于验证”在第 104 页
- “关于部署”在第 104 页

4.8.1 关于导入

可以使用导入功能导入一组现有的定义。在以下情况下需要进行导入：

- 要根据已部署的项目新建项目。

- 要与处理同一项目的其他开发者共享定义。例如，另一位开发者将一个特性添加到用户实体中，或添加新的全局列表。如果这位开发者将新定义部署到 Identity Vault 中，您可以导入此定义，这样就确保两人所使用的定义相同。

要导入现有的定义，请执行以下操作：

1 打开 《供应视图》。

2 确定要导入的内容：
   - 整个定义集
   - 某种定义类型的定义集，例如，所有实体或所有关系。
   - 一个特定对象 （例如用户实体）

3 要进行导入，请执行以下操作：
   - 一个特定对象，从列表中选择该对象，单击右键并选择 《导入对象》。
   - 整个定义集，选择 《目录提取层》节点，单击右键并选择 *Import All* （全部导入）或 《导入对象》。

4 单击 eDirectory 《浏览》图标并导航至 DirectoryModel 节点，选择要导入的对象，然后单击 《确定》。
   - 如果对象匹配，将通知您没有差异，不进行导入。
   - 如果对象不匹配，可以确认要导入的对象。审阅选定要导入的项目，进行必要的更改，然后单击 《确定》。

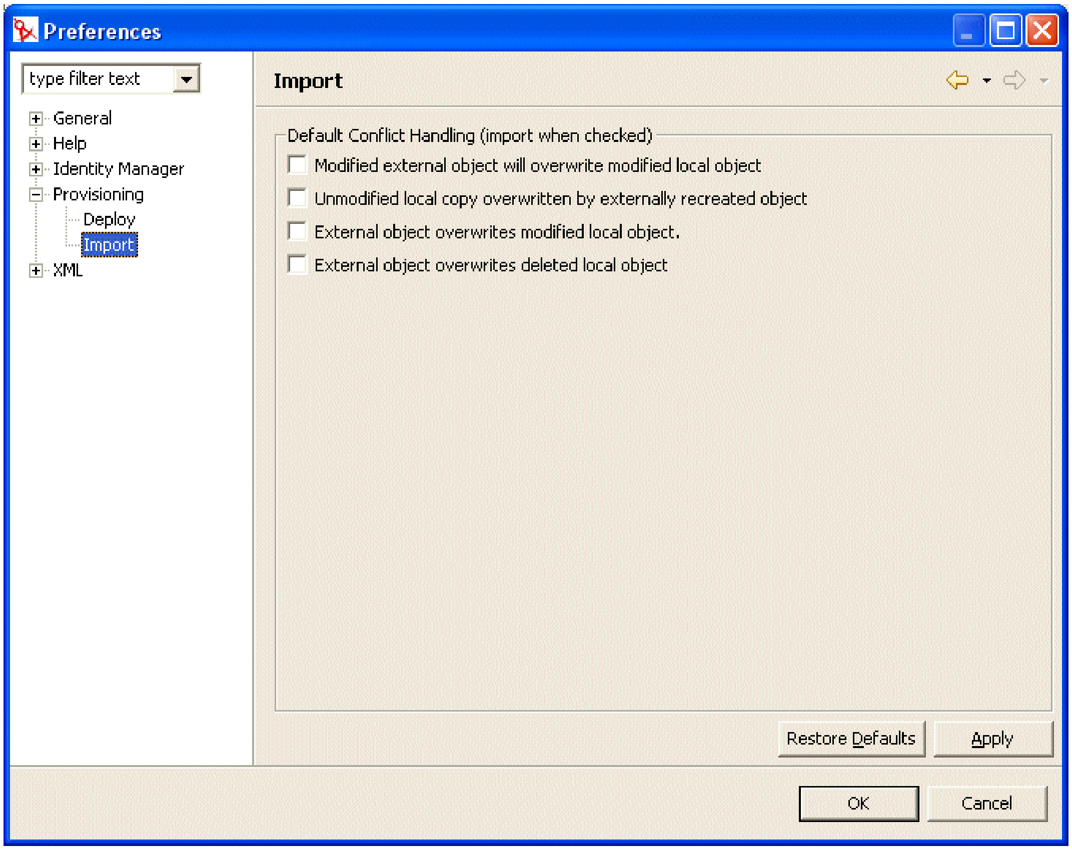
设置导入自选设置

可以使用导入自选设置指定设计程序如何解决 Identity Vault 中的数据和本地目录提取层文件数据之间的冲突。这些冲突产生的原因是不同的用户和工具都可以访问 Identity Vault 目录提取层定义。其他管理员或开发者可以使用 iManager 工具或使用他们在设计程序中自行创建的本地项目更改这些定义。如果本地文件系统定义和 Identity Vault 定义发生冲突，可以使用这些自选设置指定如何处理冲突。

要设置导入自选设置，请执行以下操作：

1 选择 《窗口》 > 《自选设置》。

2 打开树中的 《供应》节点并单击 《导入》。



3 选择自选设置：

自选设置	说明
Modified external object will overwrite modified local object （已修改的外部对象将覆盖已修改的本地对象）	本地文件和 Identity Vault 定义中都包含更改。尚未部署本地更改。 如果希望 Identity Vault 对象覆盖对本地文件所做的更改，请选择此选项。
Unmodified local copy overwritten by externally recreated object （外部重创建对象覆盖未修改的本地拷贝）	删除 Identity Vault 对象然后重创建该对象。本地文件集中包括未进行更改的原始定义。 如果希望导入内容覆盖本地拷贝，请选择此选项。
External object overwrites modified local object （外部对象覆盖已修改的本地对象）	本地文件中包含未部署到 Identity Vault 中的更改。如果希望导入时覆盖本地文件，请选择此选项。
External object overwrites deleted local object （外部对象覆盖已删除的本地对象）	已在本地删除定义，但尚未部署更改。这意味着此对象仍在 Identity Vault 中。 如果希望将 Identity Vault 中的对象复制到本地文件系统，请选择此选项。如果选择此选项，未部署的更改将丢失。

4.8.2 关于验证

可以在尝试部署目录提取层数据定义之前，在本地文件系统中验证它们。验证包括：

- 检查 XML 格式是否正确，是否符合定义实体、特性、列表、关系等所需要素的纲要。
- 检查每个实体，确保对其它实体和全局列表的参照有效。

例如，验证实体及其特性时，验证程序通过 《编辑实体》、《DN 查找》和 《细节实体》字段中实际存在的参照实体检查其它实体的所有参照。

- 确保每个实体至少定义了一个特性。
- 确保每个本地列表和全局列表中都至少包含一个项目。

可在 《供应视图》中有选择地验证定义。要验证：

- 节点中的所有项目，选择此节点，单击右键并选择 《验证》。
- 节点中的一个对象，选择此对象，单击右键并选择 《验证》。

单击目录提取层工具栏中的 *Validate Abstraction Layer* （验证提取层）按钮，可以验证所有定义。

注释 **:** 此验证不检查 Identity Vault 中是否存在对象。

4.8.3 关于部署

要想在 Identity Manager 用户应用程序中看到更改结果，必须先将定义部署到 Identity Vault 中。

要将一组定义部署到 Identity Vault，请执行以下操作：

1 使用目录提取层编辑器保存所做的全部更改。

如果在尝试部署前未保存更改，编辑器将显示一个对话框，其中显示尚未保存的定义，并提示保存最近所做的更改。如果未保存更改，也可将此对象部署到服务器，但部署的内容不包括未保存的更改。选择不保存更改不会取消部署。

2 打开 《供应视图》。

3 决定是否部署用目录提取层编辑器或子集定义的所有对象。

- 要全部部署，请执行以下操作：

  选择根节点，单击右键并选择 *Deploy All* （全部部署）
- 要部署特定的实体、关系、列表或配置设置，请执行以下操作：

  选择要部署的特定对象，单击右键并选择 《部署对象》。

系统会提示输入 Identity Vault 身份凭证。编辑器将执行验证，并在对话框中显示验证讯息。可通过选择 / 取消选择要部署的项目，来响应验证讯息。在进行完部署选择并将其提交后，将得到部署成功或失败的通知。

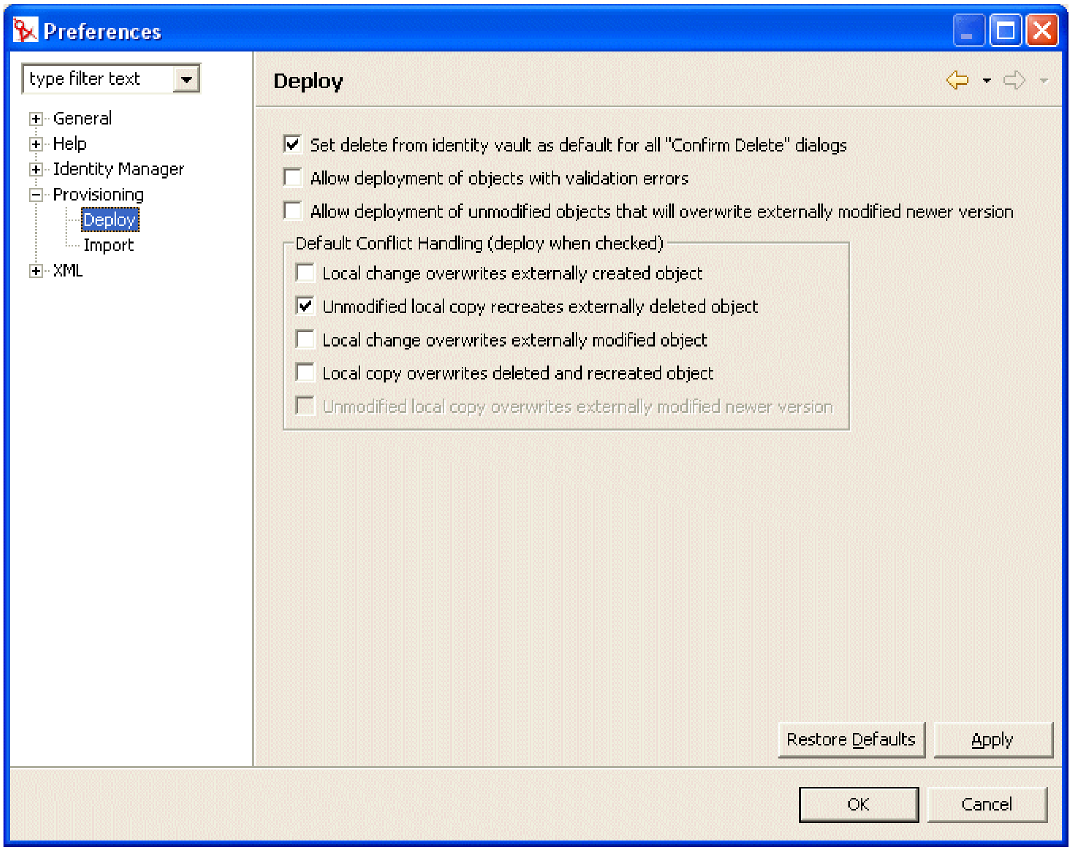
设置部署自选设置

可以使用部署自选设置指定设计程序如何解决 Identity Vault 中的数据和本地目录提取层文件数据之间的冲突。冲突产生的原因可能是：其他用户已将更改部署到 Identity Vault，但这些

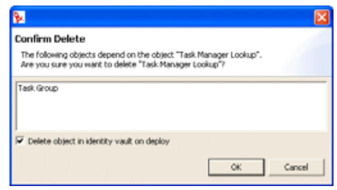
更改并未反映到您的本地文件系统定义中。要确保以预期的方法处理冲突，可以设置自选设置指定冲突解析。

要设置部署自选设置，请执行以下操作：

1 选择 《窗口》 > 《自选设置》。
2 打开树中的 《供应》节点并单击 《部署》。



3 指定一般部署自选设置：

自选设置	说明
Set delete from identity vault as default for all "Confirm Delete" dialogs （将所有 " 确认删除 " 对话框中的从 Identity Vault 中删除设为默认）	如果尝试在供应视图或目录提取层编辑器中删除对象，系统将使用如下对话框提示确认删除：  此自选设置确定在默认情况下，是否选择 **Delete object in identity vault on deploy** （部署时删除 Identity Vault 中的对象）删除确认对话框复选框。选择此自选设置意味着默认情况下将删除 Identity Vault 对象。 始终删除本地对象。
Allow deployment of objects with validation errors （验证出错时允许部署对象）	**选中** - 如果想要部署未通过验证的对象，请选择此选项。部署时，设计程序按照 “导入、验证和部署目录提取层定义” 在第 101 页 中描述的验证规则验证被部署的定义。 **取消选中** - 防止部署未通过验证的定义。
Allow deployment of unmodified objects that will overwrite externally modified newer version （允许部署将覆盖外部已修改较新版本的未修改对象）	**选中** - 如果尚未更改本地文件，但已更改 Identity Vault 对象。希望用本地文件覆盖 Identity Vault 文件吗？ 如果是，选择此自选设置。 **取消选中** - 如果希望保留较新的 Identity Vault 版本。 选中后，也可以选择冲突解析自选设置 **Unmodified local copy overwrites externally modified newer version** （未修改的本地拷贝覆盖外部已修改的较新版本）将此设为默认操作。

4 指定冲突解析自选设置：

自选设置	说明
Local change overwrites externally created object （本地更改覆盖外部创建对象）	**选中** - 如果希望用正在部署的对象覆盖 Identity Vault 中的对象。 **取消选中** - 发生此冲突时，不进行部署。
Unmodified local copy recreates externally deleted object （未修改的本地拷贝重创建外部已删除对象）	**选中** - 如果希望正在部署的本地对象创建已从 Identity Vault 中删除的对象。 **取消选中** - 发生此冲突时，不进行部署。
Local change overwrites externally modified object （本地更改覆盖外部已修改对象）	**选中** - 如果希望 Identity Vault 被另一用户更改后，仍部署本地定义。 **取消选中** - 发生此冲突时，不进行部署。
Local copy overwrites deleted and recreated object （本地拷贝覆盖已删除和重创建的对象）	**选中** - 如果希望 Identity Vault 对象被删除或被删除并重创建后，仍部署本地对象。 **取消选中** - 发生此冲突时，不进行部署。

自选设置	说明
Unmodified local copy overwrites externally modified newer version （未修改的本地拷贝覆盖外部已修改的较新版本）	只能在一般部署自选设置中选中 **Allow deployment of unmodified objects that will overwrite externally modified newer version** （允许部署将覆盖外部已修改较新版本的未修改对象）后，才可设置此自选设置。 **选中** - 如果未更改本地文件，但已更改 Identity Vault 对象，并始终希望默认操作为本地文件覆盖 Identity Vault 文件。 **取消选中** - 如果希望保留较新的 Identity Vault 版本。

设置日志记录 5

本章包括以下内容：

5.1 关于事件日志记录

Identity Manager 用户应用程序使用由 Apache Software Foundation 分发的开放源代码日志记录包 *log4j* 实施日志记录。默认情况下，事件讯息会记录到系统控制台和应用程序服务器的日志文件中，日志记录级别为 INFO 及以上。也可将用户应用程序配置为记录到 Novell Audit。事件将记录到全部激活的记录器中。

重要：如果记录到 Novell Audit，建议审阅 Novell Audit 文档 (http://www.novell.com/documentation/nsureaudit)。

5.1.1 关于日志级别设置

控制台日志记录包括同步写入。这意味着日志记录可以成为处理程序使用问题和并发阻抗。可以修改 <*installdir*>/jboss/server/IDMProv/conf/log4j.xml 中的设置，将优先级值默认设置更改为 ERROR。找到如下根节点：

```
<root> <appender-ref ref="CONSOLE"/> <appender-ref ref="FILE"/> </
root>
```

将优先级值更改为：

```
<root> <priority value="ERROR"/> <appender-ref ref="FILE"/> </root>
```

为根赋值，可确保没有显式指派级别的所有附加程序都可以继承根的级别。默认情况下，由于文件附加程序没有指派的阈值级别，因此继承根的级别。根中包括的所有日志信息输出目的地的级别阈值均为 ERROR 或 WARN。将错误级别设置为高于 WARN 将影响性能。

5.2 记录到 Novell Audit 服务器

要记录到 Novell Audit 服务器，请执行以下步骤：

步骤	操作	详细信息
1	将 Identity Manager 应用程序纲要作为日志应用程序添加到 Novell Audit 服务器中	“将 Identity Manager 应用程序纲要作为日志应用程序添加到 Novell Audit 服务器中”在第 110 页

步骤	操作	详细信息
2	在应用程序服务器上配置 Novell Audit 平台代理	任何向 Novell Audit 报告事件的客户机都需要平台代理。平台代理通过 **logevent configuration** 文件进行配置。该文件提供平台代理与 Novell Audit 服务器进行通讯所需的配置信息。它在应用程序服务器上的默认位置为： ◆ Linux - /etc/logevent.conf ◆ Windows - /<WindowsDir>/logevent.cfg（通常为 c:\windows） 请确保已在 **LogHost** 设置中指定了 **Novell Audit 服务器的 IP 地址或 DNS 名称**。例如： `LogHost=xxx.xxx.xxx.xxx` 指定环境所需的任何其它设置。 **重要 :** 在创建或修改 logevent 配置文件后，必须重启动 JBoss 应用程序才能使这些更改生效。 有关 logevent 配置文件结构的更多信息，请参见《Novell Audit 管理指南》中有关日志记录系统一章的配置平台代理 (http://www.novell.com/documentation/nsureaudit) 部分。
3	启用 Novell Audit 日志记录	“启用 Audit 日志记录”在第 111 页

5.2.1 将 Identity Manager 应用程序纲要作为日志应用程序添加到 Novell Audit 服务器中

若要将 Audit 配置为将 Identity Manager 用户应用程序用作日志应用程序，请按照下列步骤操作：

1 找到以下文件：

```
DirXML.lsc
```

平台	位置
Linux	安装后： `/opt/novell/naudit/logschema/dirxml.lsc`

平台	位置
Windows	在安装媒体上： /nt/dirxml/nsure_audit/nauditextensions/lsc/ dirxml.lsc

2 使用万维网浏览器访问 *iManager*，然后以管理员身份登录。

3 转至 *Roles and Tasks* > *Auditing and Logging* （职能和任务 > 审计和日志记录），然后选择 *Logging Server Options* （日志记录服务器选项）。

4 通过浏览找到树中的日志记录服务树枝，选择适当的 *Audit* 安全性日志记录服务器。然后单击 《确定》。

5 转至 *Log Applications* （日志应用程序）选项卡，选择适当的 《树枝名称》，然后单击 *New Log Application* （新建日志应用程序）链接。

6 显示 《新建日志应用程序》对话框时，请指定以下内容：

设置	操作
日志应用程序名	键入对环境有意义的任何名称
导入 LSC 文件	使用 《浏览》按钮选择 **DirXML.lsc** 文件

然后单击 《确定》。 《日志应用程序》选项卡将显示已添加的应用程序名。

7 单击 《确定》完成 Novell Audit 服务器配置。

8 请确保将 《日志应用程序》的状态设置为 《开》。 （状态下方的圆圈应为绿色。若为红色，请通过单击将其切换为 《开》。）

9 重启动 Novell Audit 服务器以激活新的日志应用程序设置。

5.2.2 启用 Audit 日志记录

在 Identity Manager 用户应用程序中启用 Novell Audit 日志记录

1 以 Admin 用户的身份登录该用户应用程序。

2 选择 《管理》选项卡。

3 选择 《日志记录》选项卡。

4 选中 《同时向 Audit 发送日志记录讯息》复选框 （接近选项卡底部）。

5 为确保应用程序服务器在任何后续重启动后都保持这些更改，请确保已选中 《保持日志记录更改》。

5.2.3 已记录的事件

Identity Manager 用户应用程序会自动日志记录工作流程、搜索、细节和口令请求中的一系列事件。默认情况下， Identity Manager 用户应用程序会自动向所有活动的日志记录通道记录以下事件：

事件 ID	进程	事件	严重性
31400	细节入口小程序	Delete_Entity	信息
31401		Update_Entity	信息
31410	更改口令入口小程序	Change_Password_Failure	错误
31411		Change_Password_Success	信息
31420	忘记口令入口小程序	Forgot_Password_Change_Failure	错误
31421		Forgot_Password_Change_Success	信息
31430	搜索入口小程序	Search_Request	信息
31431		Search_Saved	信息
31440	创建入口小程序	Create_Entity	信息
31520	工作流程	Workflow_Error	错误
31521		Workflow_Started	信息
31522		Workflow_Forwarded	信息
31523		Workflow_Reassigned	信息
31524		Workflow_Approved	信息
31525		Workflow_Refused	信息
31526		Workflow_Ended	信息
31527		Workflow_Claimed	信息
31528		Workflow_Unclaimed	信息
31529		Workflow_Denied	信息
3152A		Workflow_Completed	信息
3152B		Workflow_Timedout	信息
3152C		User_Message	信息
31533		Workflow_Retracted	信息
3152D	供应	Provision_Error	错误
3152E		Provision_Submitted	信息
3152F		Provision_Success	信息
31530		Provision_Failure	错误
31531		Provision_Granted	信息
31532		Provision_Revoked	信息

事件 ID	进程	事件	严重性
31450	安全环境	Create_Proxy_Definition_Success	信息
31451		Create_Proxy_Definition_Failure	错误
31452		Update_Proxy_Definition_Success	信息
31453		Update_Proxy_Definition_Failure	错误
31454		Delete_Proxy_Definition_Success	信息
31455		Delete_Proxy_Definition_Failure	错误
31456		Create_Delegatee_Definition_Success	信息
31457		Create_Delegatee_Definition_Failure	错误
31458		Update_Delegatee_Definition_Success	信息
31459		Update_Delegatee_Definition_Failure	错误
3145A		Delete_Delegatee_Definition_Success	信息
3145B		Delete_Delegatee_Definition_Failure	错误
3145C		Create_Availability_Success	信息
3145D		Create_Availability_Failure	错误
3145E		Delete_Availability_Success	信息
3145F		Delete_Availability_Failure	错误

5.2.4 日志报告

如果将事件记录在 Novell Audit 数据库通道中，则可以对该数据运行报告。对已记录在 Novell Audit 数据库中的数据生成报告存在多种方法：

- 使用 Novell Audit Report 应用程序运行自己的报告，或运行下面 "预定义的日志报告" 在第 113 页 中描述的预定义报告。
- 通过在 iManager 中选择 《审计和日志记录》 > 《查询》对已记录的数据编写查询。
- 对已记录的数据编写自己的 SQL 查询。

默认的 Novell Audit 表称为 NAUDITLOG。

预定义的日志报告

以下预定义的日志报告以 Crystal Reports (*.rpt*) 格式创建，用于过滤已记录到 Novell Audit 数据库中的数据：

报告名称	说明
管理操作报告	显示 Identity Manager 用户应用程序入口中启动的所有管理操作。该报告包含启动操作的管理员。 它不包括使用 iManager 或 IDM 设计程序进行的任何管理更改
历史批准流程报告	显示指定时间范围内的所有批准流程活动。

报告名称	说明
资源供应报告	显示按资源排序的所有供应活动。
特定用户审计追踪	显示与用户相关的所有活动。其中包括供应和自助服务两类活动。
特定用户供应报告	显示特定用户的所有供应活动。
用户供应报告	显示按用户排序的所有供应活动。

报告样本 此样本是特定用户审计追踪的一个示例：

Novell® Audit Report for Identity Manager

Specific User Audit Trail

Report Period: - 10/13/2005 8:51:32AM

User ID: ablake

Report Last Modified: 10/13/2005
Report Generated On: 10/13/2005
Total pages: 8

Approval Flow

Workflow Event: fecedbe80a3d4abd83c9476a1b576ea2

Date / Time	Action	Initiator ID
9/12/2005 3:20:42PM	Workflow Started	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/12/2005 3:20:43PM	Workflow Forwarded	Workflow Administrator
9/12/2005 3:25:43PM	Workflow Reassigned	Unclaimed
9/12/2005 3:30:44PM	Workflow Forwarded	Workflow Administrator
9/12/2005 3:30:44PM	Workflow Ended	Workflow Administrator
9/12/2005 3:30:44PM	Workflow Denied	System

Workflow Event: fc6d74b1268243b3beac52261439dea0

Date / Time	Action	Initiator ID
9/28/2005 1:12:19PM	Workflow Started	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 1:12:22PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Approved	System
9/28/2005 2:12:23PM	Workflow Approved	System
9/28/2005 2:12:23PM	Workflow Completed	Workflow Administrator
9/28/2005 2:12:27PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:27PM	Workflow Ended	Workflow Administrator
9/28/2005 2:12:27PM	Provision Submitted	Workflow Administrator
9/28/2005 2:12:27PM	Provision Granted	Workflow Administrator

Workflow Event: efaa8304e07641edb9e6375a1a36e396

Date / Time	Action	Initiator ID
10/12/2005 11:58:13AM	Workflow Started	cn=ablake,ou=users,ou=idmsample-qatest,o=novell
10/12/2005 11:58:13AM	Workflow Forwarded	Workflow Administrator

Workflow Event: ea341eb11a824e669e356837745fe264

Date / Time	Action	Initiator ID
9/27/2005 4:24:44PM	Workflow Started	cn=mmackenzie,ou=users,ou=idmsample-Jeff,o=novell
9/27/2005 4:24:44PM	Workflow Forwarded	Workflow Administrator

Page 1 of 8 Specific User Audit Trail

报告文件位置 报告文件位于：

平台	位置
Windows	/nt/dirxml/reports

可以将这些报告用作在 Crystal Reports 设计程序中创建自定义报告的模板，也可以使用 Novell Audit 附带的 Windows 程序 *Audit Report* (lreport.exe) 运行它们。预定义报告从默认的 Novell Audit 日志数据库（名为 *naudit* ）和名为 *nauditlog* 数据库表中查询数据。如果 Novell Audit 日志数据库具有不同的名称，请使用 Crystal Reports 设计程序中的 *Set Datasource Location* （设置数据源位置）菜单项将 *naudit* 数据库名替换成特定环境中相应的名称。

有关更多信息，请参见 Novell Audit 文档 (http://www.novell.com/documentation/nsureaudit) 中有关使用报告的部分。

管理用户应用程序

III

以下几章将说明如何使用用户界面中的 《管理》选项卡来配置和管理 Identity Manager 用户应用程序。

使用 《管理》选项卡 6

本章将介绍 Identity Manager 用户界面上的 《管理》选项卡。可以从中了解如何使用 《管理》选项卡来配置和管理 Identity Manager 用户应用程序。包括以下主题：

6.1 关于 《管理》选项卡

Identity Manager 用户界面主要由终端用户访问，他们使用界面中提供的选项卡进行身份自助服务和基于流程的供应 （通过 Identity Manage 的预置模块）。但这一基于浏览器的用户界面还提供了一个 《管理》选项卡。管理员可访问该选项卡并在其中配置 Identity Manager 用户应用程序的各种基本特征。

例如：《管理》选项卡可用于：

- 更改用于控制用户界面外观的主题
- 自定义可供终端用户使用的身份自助服务功能
- 指定允许执行管理操作的人员
- 管理有关此用户应用程序及其运行方式有关的其它细节

6.2 有权使用 《管理》选项卡的人员

Identity Manager 用户界面的某些典型终端用户无法看到 《管理》选项卡。可以看到并访问该选项卡的用户包括以下两类：

- 用户应用程序管理员

  用户应用程序管理员有权执行与 Identity Manager 用户应用程序相关的所有管理功能。其中包括通过访问 Identity Manager 用户界面的 《管理》选项卡来执行其支持的所有管理操作。

  在安装过程中，指定了作为用户应用程序管理员的用户。安装完成后，该用户将可以使用 《管理》选项卡中的 《安全性》页，在需要时指定其他用户应用程序管理员。

  有关详情，请参见第 11 章 “安全性配置”在第 189 页 。
- 用户应用程序管理员批准的用户

  如有必要，用户应用程序管理员可以将许可权限指派给一个或多个终端用户，使其可以查看并访问 《管理》选项卡上的特定页。使用 《管理》选项卡中的 《页管理》页可指派这些许可权限。

  有关详情，请参见第 7 章 “页管理”在第 125 页 。

6.3 访问 《管理》选项卡

成为用户应用程序管理员 （或其他获准用户）后，可以在需要管理 Identity Manager 用户应用程序时访问 Identity Manager 用户界面中的 《管理》选项卡。只需要安装一个受支持的万维网浏览器。

有关受支持的万维网浏览器的列表，请参见 《*Novell Identity Manager*：安装指南》。

注释 **:** 若要使用 Identity Manager 用户界面，请确保万维网浏览器已启用了 *JavaScript*。

要访问 《管理》选项卡，请执行以下操作：

1 在万维网浏览器中，转至 （站点中配置的） Identity Manager 用户界面的 URL。例如：

```
http://myappserver:8080/IDM
```

将显示该用户界面的迎宾页：



2 单击页标题中的 《登录》链接。

用户界面将提示输入用户名和口令：



3 输入用户应用程序管理员 （或具有部分 《管理》选项卡许可权限的用户）的用户名和口令，然后单击 《登录》。

登录后，可以看到针对该用户的相应用户界面内容。例如：



默认情况下显示 《身份自助服务》选项卡。

4 单击 《管理》选项卡。

《管理》选项卡将显示一个可以执行的管理操作的菜单。每选择一种操作都将显示相应的设置和控件页。默认情况下，可以看到 《页管理》页：



有关访问和使用 Identity Manager 用户界面的更多一般信息，请参见 《*Identity Manager* 用户应用程序：用户指南》。

6.4 可以执行的管理操作

在 《管理》选项卡中，可以使用所有可用操作来配置和管理 Identity Manager 用户应用程序。下面简要说明了这些操作：

操作	说明
页管理	控制 Identity Manager 用户界面中显示的页以及有权进行访问的用户 有关详情，请参见第 7 章 “页管理” 在第 125 页 。
主题	控制 Identity Manager 用户界面的外观 有关详情，请参见第 8 章 “主题配置” 在第 159 页 。
入口小程序管理	控制 Identity Manager 用户界面上可用的入口小程序以及有权访问它们的人员 有关详情，请参见第 9 章 “入口小程序管理” 在第 165 页 。
入口	控制 Identity Manager 用户应用程序的入口特征，并指定该用户应用程序与 Identity Vault （LDAP 提供程序）的连接方式 有关详情，请参见第 10 章 “入口配置” 在第 183 页 。
安全性	指定谁是 Identity Manager 用户应用程序的用户应用程序管理员 有关详情，请参见第 11 章 “安全性配置” 在第 189 页 。
日志记录	控制希望 Identity Manager 用户应用程序生成的日志记录讯息的级别，并指定是否将这些讯息发送到 Novell Audit 有关详情，请参见第 12 章 “日志记录配置” 在第 193 页 。

操作	说明
超速缓存	管理 Identity Manager 用户应用程序维护的各种超速缓存 有关详情，请参见第 13 章 “超速缓存配置”在第 199 页 。
工具	用于导出或导入 Identity Manager 用户应用程序使用的入口内容 （页和入口小程序） 有关详情，请参见第 14 章 “用于导出和导入入口数据的工具”在第 207 页 。

页管理 7

本章将说明如何使用 Identity Manager 用户界面上 《管理》选项卡的 《页管理》页。包括以下主题：

- “关于页管理”在第 125 页
- “创建并维护树枝页”在第 132 页
- “创建并维护共享页”在第 140 页
- “指派页的许可权限”在第 148 页
- “设置组的默认页”在第 154 页
- “为树枝页选择默认共享页”在第 156 页

有关访问和使用 《管理》选项卡的更多一般信息，请参见第 6 章 “使用 《管理》选项卡”在第 119 页 。

7.1 关于页管理

使用 《页管理》页可以控制显示在 Identity Manager 用户界面上的页，以及有权 访问它们的人员。该用户界面包括两种类型的页：

页类型	说明
树枝	树枝页以一致的外观、公司商标和导航方法包装共享页。
共享	共享页提供一组用于特定用途 （如更新用户简报）的一致内容。由于它们提供的服务可供多人使用，因此被称为共享页。

这两种页都包含形式为入口小程序 （可插用户界面要素的一种 Java 标准）的内容。

若要了解有关入口小程序的更多信息，请参见第 9 章 “入口小程序管理”在第 165 页 和“入口小程序参照”在第 215 页 。

7.1.1 关于树枝页

本部分将介绍 Identity Manager 用户界面中的一些重要树枝页：

- “GuestContainerPage （访客树枝页）”在第 126 页
- “DefaultContainerPage （默认树枝页）”在第 128 页
- “管理树枝页”在第 129 页

请记住，如有必要，可以修改这些树枝页。还可以添加自己的树枝页。

若要了解有关使用树枝页的信息，请参见 “创建并维护树枝页”在第 132 页 。

GuestContainerPage（访客树枝页）

默认情况下，当用户在登录前访问 Identity Manager 用户界面时，他们将看到名为 *GuestContainerPage* 的树枝页。该树枝页显示如下：



GuestContainerPage 的内部布局如下：



GuestContainerPage 布局分为三个区域，其中显示以下入口小程序：

入口小程序	说明
HeaderPortlet	显示用户界面的标题信息和顶级选项卡控件
共享页导航	显示了一个垂直菜单，用户可以从中选择要显示的共享页
入口页控制器	显示用户当前通过 《共享页导航》入口小程序选择的共享页

请注意，在默认情况下，用户在登录前只能在这些入口小程序中看到以下内容：

- 一个页眉中的链接：登录
- 一个共享页：欢迎

由于用户尚未登录，《共享页导航》入口小程序将仅显示 《Guest 页》类别的共享页，而将其他类别的共享页都排除在外。默认情况下，《欢迎》页是 《Guest 页》类别的唯一页。

登录后，《共享页导航》入口小程序会将 《Guest 页》类别排除在外，而是显示其它类别的共享页 （在共享页自选设置中指定）。

有关 《共享页导航》入口小程序的更多信息，请参见第 15 章 “关于入口小程序”在第 217 页 。

DefaultContainerPage （默认树枝页）

默认情况下，在用户登录到 Identity Manager 用户界面之后，他们将转到名为 *DefaultContainerPage* 的树枝页。该树枝页显示如下：



DefaultContainerPage 的内部布局如下：



DefaultContainerPage 布局分为三个区域，其中显示以下入口小程序：

入口小程序	说明
HeaderPortlet	显示用户界面的标题信息和顶级选项卡控件
共享页导航	显示了一个垂直菜单，用户可以从中选择要显示的共享页
入口页控制器	显示用户当前通过 《共享页导航》入口小程序选择的共享页
会话超时警告	在用户会话即将超时时显示一条警报讯息

请注意，在用户登录后， *DefaultContainerPage* 将自动打开 *HeaderPortlet* 中的 《身份自助服务》选项卡。

管理树枝页

默认情况下，当用户应用程序管理员 （及其他已授权用户）单击 *Identity Manager* 用户界面的 《管理》选项卡 后，他们将转到名为 《管理树枝页》的树枝页。该树枝页显示如下：



《管理树枝页》的内部布局如下：



《管理树枝页》的布局分为两个区域，其中将显示以下入口小程序：

入口小程序	说明
HeaderPortlet	显示用户界面的标题信息和顶级选项卡控件
管理列表显示	显示二级选项卡，用户可以从中选择要执行的管理操作
入口页控制器	显示一个共享页，该页对应于用户当前通过 《管理列表显示》入口小程序选择的选项卡
会话超时警告	在用户会话即将超时时显示一条警报讯息

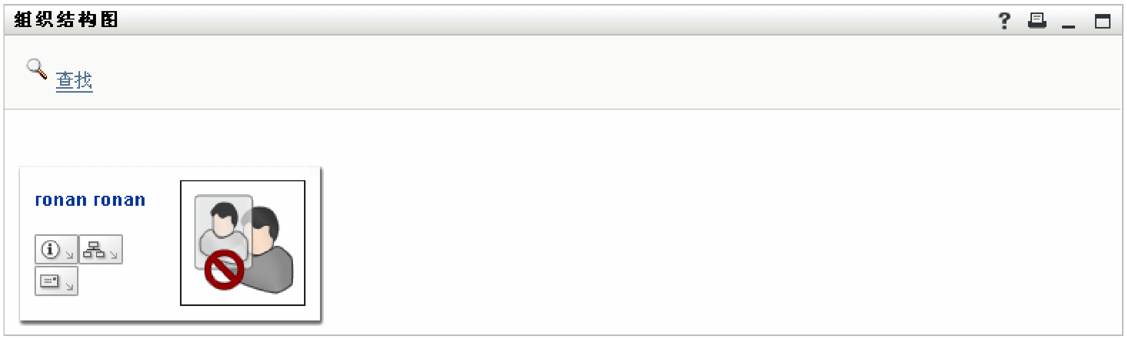
7.1.2 关于共享页

Identity Manager 用户界面包含许多共享页，它们提供了界面中树枝页的主要内容。可以对这些共享页进行必要的修改，还可以添加自己的共享页。

若要了解使用共享页的信息，请参见 “创建并维护共享页”在第 140 页 。

典型的共享页

让我们来看看其中的一个共享页。《组织结构图》是在用户登录到 Identity Manager 用户界面后， DefaultContainerPage 默认显示的共享页。



《组织结构图》的内部布局如下：



《组织结构图》布局仅包含一个区域，其中仅显示一个入口小程序 （《组织结构图》入口小程序）。

7.1.3 不使用页的情况

本章已经介绍了 Identity Manager 用户界面中的这些顶级选项卡如何基于页：

- 《身份自助服务》选项卡使用 *DefaultContainerPage*
- 《管理》选项卡使用 《管理树枝页》

但请注意，《请求和批准》选项卡基于不同的体系结构，无法通过 《页管理》进行处理。

7.2 创建并维护树枝页

创建和维护树枝页的过程包括以下步骤：

1. 创建一个新的树枝页或选择一个现有的树枝页，如 "创建树枝页"在第 132 页 中所述。
2. 向页中添加内容 （以入口小程序的形式），如 "向树枝页中添加内容"在第 135 页 中所述。

   如果还希望从页中删除内容，则可以按照 "删除树枝页中的内容"在第 136 页 中所述的方法操作。
3. 选择入口布局，如 "修改树枝页的布局"在第 137 页 中所述。
4. 在所选布局上排列内容的顺序和位置，如 "排列树枝页上的内容"在第 138 页 中所述。
5. 通过在浏览器中输入树枝页的 URL 立刻显示新页，如 "显示树枝页"在第 140 页 中所述。

树枝页及布局 树枝页并未紧密联结到入口布局。这意味着，可以切换树枝页的布局，而不会丢失任何页面内容。对树枝页应用新的布局时，所有添加到该页的入口小程序都将自动以新的布局显示。可能需要在新布局中对内容位置进行微调。

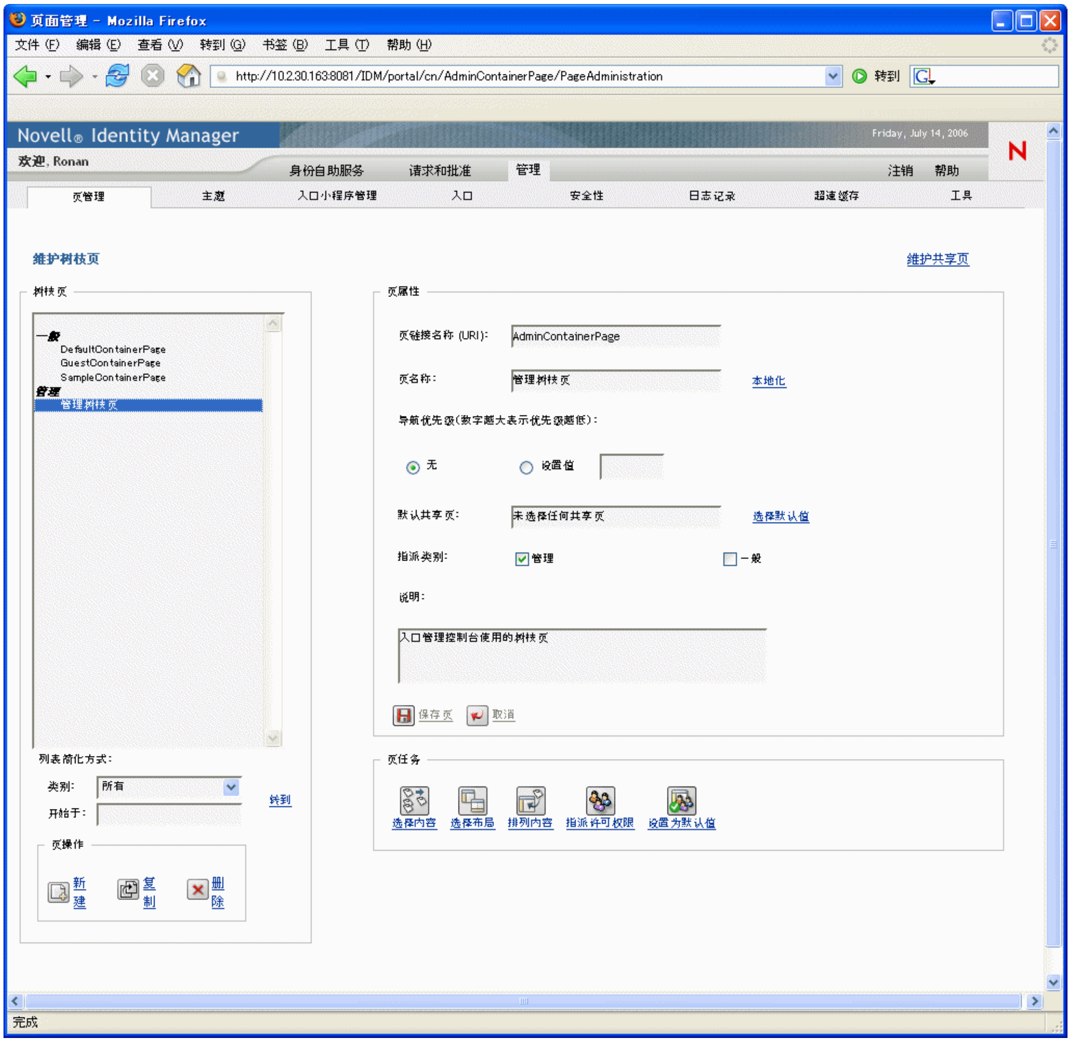
7.2.1 创建树枝页

创建树枝页时，可以从头创建，也可以通过复制现有页创建。本部分将对这两种方法进行具体介绍。

要从头创建树枝页，请执行以下操作：

1. 在 《页管理》页上，选择 《维护树枝页》。

将显示《维护树枝页》面板：



2 选择《新建》页操作（位于面板左下部）。

将创建一个无标题和类别的树枝页。

3 指定树枝页的页属性：

属性	操作

页链接名称 (URI)	指定页的 URI 名称 （将显示在用户界面 URL 中）。例如，如果指定 URI：
	
	`MyContainerPage`
	
	则它在 URL 中将显示为：
	
	`http://myappserver:8080/IDM/portal/cn/`
	`MyContainerPage`

页名称	指定页的显示名称。例如： `My Container Page` 可以单击 《本地化》，以指定此名称在其它语言中的本地化版本。
导航优先级	请指定以下项之一： ◆ 《无》 - 在不需要为该树枝页指派优先级时使用。 ◆ 《设置值》 - 为该树枝页指派一个相对于其它树枝页的优先级。优先级必须是介于 -1 到 9999 之间的整数，其中，-1 代表最高优先级， 9999 代表最低优先级。 如果希望确保页面在按优先级列出时能以某一特定的顺序显示，或希望确保在存在多个默认页时 （此时一个用户属于多个组）选择某一特定的页，则设置优先级的值将非常有用。
默认共享页	请参见 "为树枝页选择默认共享页"在第 156 页 。
指派类别	在以下类别中选择该页所属的类别 （可选）： ◆ 管理 ◆ 一般 如果希望确保合理组织按类别列出的页，或希望确保在对页按类别过滤后能得到适当的子集，则指派类别将非常有用。
说明	键入描述页的文本。

4 单击 《保存页》（位于页属性部分的底部）。

要通过复制现有页创建树枝页，请执行以下操作：

1 在 《页管理》页上，选择 《维护树枝页》。

将显示 《维护树枝页》面板 （如上一步中所示）。

2 在树枝页列表中，选择要复制的页。

提示：如果该列表较长，则可以 （按类别或起始文本）简化该列表，以便更轻易地找到所需的页。

3 选择 《复制》页操作 （位于面板左下部）。

将创建一个名为 *OriginalPageName* 拷贝的新树枝页。

4 指定树枝页的页属性 （按上一步中说明的方法）。

5 单击 《保存页》（位于页属性部分的底部）。

7.2.2 向树枝页中添加内容

创建树枝页后，下一步便是选择要放置到页中的入口小程序，以此来添加内容。可以使用 Identity Manager 用户应用程序附带的预生成入口小程序，也可以使用已经注册的其它入口小程序。

要向树枝页中添加内容，请执行以下操作：

1 在 《维护树枝页》面板中打开一个新页或现有页，然后单击 《选择内容》页任务 （位于面板底部）。

将在新的浏览器窗口中显示 《内容选择器》：



2 如果要显示特定类别的可用内容，请从 《过滤器》下拉菜单中选择类别。

3 从 《可用的内容》列表中选择一个或多个入口小程序。

提示：按住 *Ctrl* 键可从列表中选择多个不相邻的入口小程序；按住 *Shift* 键可选择多个相邻的入口小程序。

4 单击 《添加》将所选内容移动到 《选择的内容》列表中。
5 可以单击 《内容自选设置》来编辑为树枝页选择的所有入口小程序的自选设置。指定的自选设置值将应用于显示在页中的入口小程序实例。
6 单击 《保存内容》。

现在，已经为树枝页选择了内容，接下来，可以按照"修改树枝页的布局"在第 137 页中描述的方法选择一个新布局，或按照"排列树枝页上的内容"在第 138 页中描述的方法排列当前布局中的内容。

7.2.3 删除树枝页中的内容

在创建树枝页的过程中，可能需要去除页中的入口小程序从而删除内容。可以使用 《内容选择器》或 《布局选择器》，现将具体过程介绍如下。

要使用 《内容选择器》删除树枝页中的内容，请执行以下操作：

1 在 《维护树枝页》面板中打开一个页，然后单击 《选择内容》页任务 （位于面板底部）。

将在新的浏览器窗口中显示 《内容选择器》（如上一步中所示）。

2 选择要从 《选择的内容》列表中删除的入口小程序，然后单击 《去除》。

该入口小程序即从页中去除。

3 单击 《保存内容》。

要使用 《布局选择器》删除树枝页中的内容，请执行以下操作：

1 在 《维护树枝页》面板中打开一个页，然后单击 《排列内容》页任务 （位于面板底部）。

将在新的浏览器窗口中显示 《布局选择器》，其中将列出该页中的入口小程序：



2 单击要去除的入口小程序的 *X* 按钮。

3 收到确认提示时，请单击 《确定》。

该入口小程序即从页中去除。

4 单击 《保存布局》。

7.2.4 修改树枝页的布局

修改树枝页的布局时，现有内容也将调整，以适应新的布局。某些情况下，可能需要对最终结果进行微调。

要修改树枝页的布局，请执行以下操作：

1 在 《维护树枝页》面板中打开一个页，然后单击 《选择布局》页任务 （位于面板底部）。

将在新的浏览器窗口中显示 《入口布局》列表：



2 通过滚动浏览选项，并选择所需的布局。

3 单击 《选择布局》。

7.2.5 排列树枝页上的内容

为树枝页选择内容和布局之后，便可以将内容定位到所选布局之中，也可在特定位置添加或删除入口小程序。

要排列树枝页上的内容，请执行以下操作：

1 在 《维护树枝页》面板中打开一个页，然后单击 《排列内容》页任务 （位于面板底部）。

将在新的浏览器窗口中显示 《布局选择器》，其中将列出该页中的入口小程序：



2 如果要向页中添加入口小程序，请按照下列步骤操作：

2a 在所需的布局框架中单击 《添加内容》。

将在新的浏览器窗口中显示 《入口小程序选择器》。

2b 如果要显示特定类别的可用内容，请从 《过滤器》下拉菜单中选择类别。

2c 从 《可用的内容》列表中选择所需的入口小程序。

2d 单击 《选择内容》。

将关闭 《入口选择器》，并且所选择的入口小程序将显示在 《布局选择器》的目标布局框架中。

3 如果要将入口小程序移动到布局中的其它位置，请按照下列特定于浏览器的步骤进行操作：

浏览器	操作
Internet Explorer	1. 将光标移到入口小程序的标题栏上，直到光标变为手形。 2. 按住鼠标左键，将入口小程序拖到布局中的所需位置。
Mozilla	1. 单击要移动的入口小程序。 2. 在目标布局框架内单击。 入口小程序随即会移动到目标位置。

4 如果要从布局中去除入口小程序，请按照下列步骤操作：

  4a 单击要去除的入口小程序的 *X* 按钮。

  4b 收到确认提示时，请单击 《确定》。

  入口小程序将从布局中去除。

5 如果要编辑入口小程序的自选设置，请按照下列步骤操作：

  5a 单击要编辑的入口小程序的铅笔形按钮。

  浏览器中将显示入口小程序的 《内容自选设置》。

  5b 根据需要更改自选设置的值。

  指定的自选设置值将应用于显示在页中的入口小程序实例。

  5c 单击 《保存自选设置》。

6 单击 《保存布局》记录更改，然后关闭 《布局选择器》。

7.2.6 显示树枝页

在浏览器中转到树枝页的 URL 可以显示该页。

要显示树枝页，请执行以下操作：

- 在万维网浏览器中，转到以下 URL：

  `http://`*`server:port`*`/`*`IDM-war-context`*`/portal/cn/`*`container-page-name`*

  例如，若要显示名为 *MyContainerPage* 的树枝页，应转到：

  `http://myappserver:8080/IDM/portal/cn/MyContainerPage`

7.3 创建并维护共享页

创建和维护共享页的过程包括以下步骤：

1 创建一个新的共享页或选择一个现有的共享页，如 "创建共享页" 在第 141 页 中所述。

2 向页中添加内容 （以入口小程序的形式），如 "向共享页添加内容" 在第 143 页 中所述。

  如果还希望从页中删除内容，则可以按照 "删除共享页中的内容" 在第 145 页 中所述的方法操作。

3 选择入口布局，如 "修改共享页的布局" 在第 146 页 中所述。

4 在所选布局上排列内容的顺序和位置，如 "排列共享页中的内容" 在第 147 页 中所述。

5 通过在浏览器中输入共享页的 URL 立刻显示新页，如 "显示共享页" 在第 148 页 中所述。

共享页及布局 共享页并未紧密联结到入口布局。这意味着，可以切换共享页的布局，而不会丢失任何页面内容。对共享页应用新的布局时，所有添加到该页的入口小程序都将自动以新的布局显示。可能需要在新布局中对内容位置进行微调。

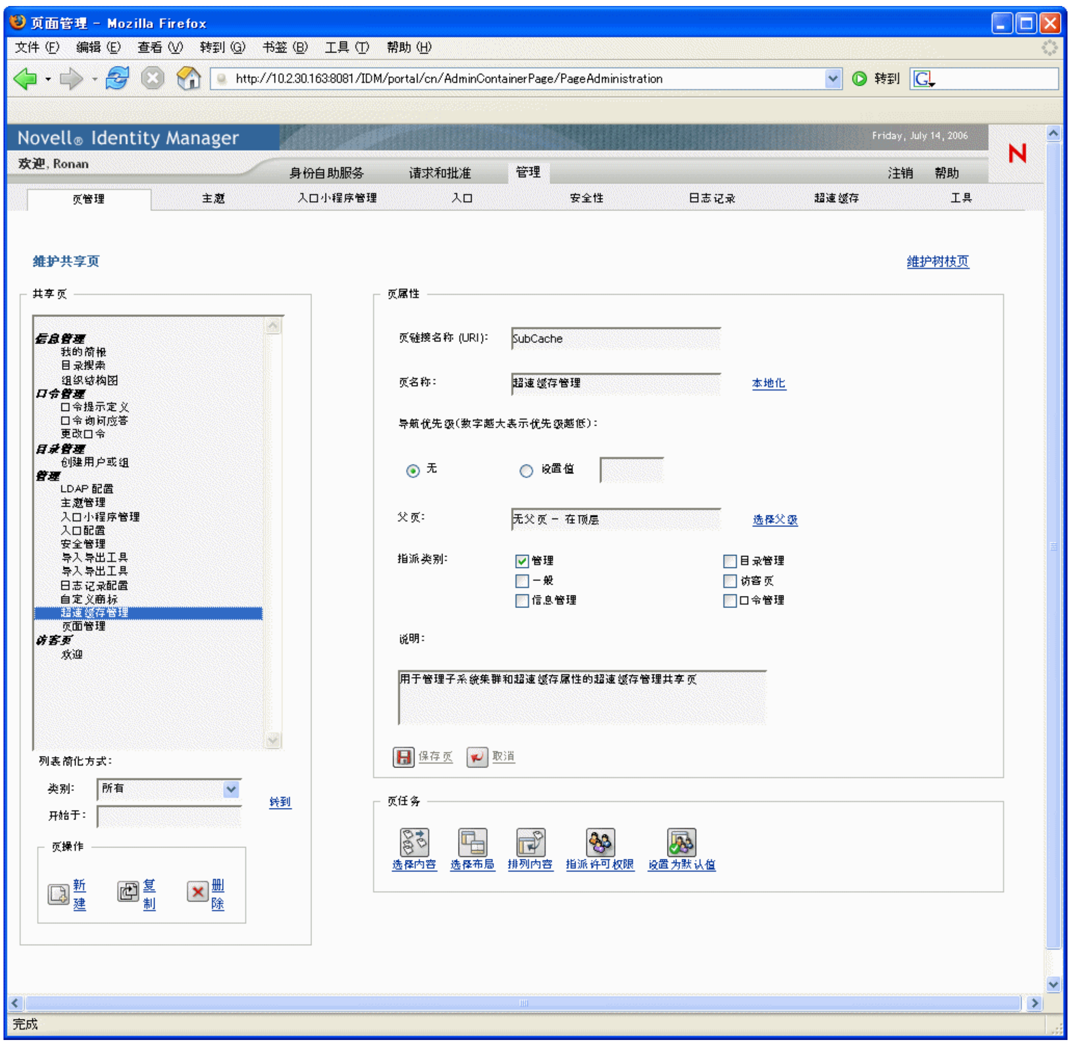
7.3.1 创建共享页

创建共享页时，可以从头创建，也可以通过复制现有页创建。本部分将对这两种方法进行具体介绍。

要从头创建共享页，请执行以下操作：

1 在 《页管理》页上，选择 《维护共享页》。

将显示 《维护共享页》面板：



2 选择 《新建》页操作 （位于面板左下部）。

将创建一个无标题和类别的共享页。

3 指定共享页的页属性：

属性	操作
页链接名称 (URI)	指定页的 URI 名称 （将显示在用户界面 URL 中）。例如，如果指定 URI： `MySharedPage` 则它在 URL 中将显示为： `http://myappserver:8080/IDM/portal/cn/MyContainerPage/`**`MySharedPage`**
页名称	指定页的显示名称。例如： `My Shared Page` 可以单击 《本地化》，以指定此名称在其它语言中的本地化版本。
导航优先级	请指定以下项之一： ◆ 《无》 - 在不需要为该共享页指派优先级时使用。 ◆ 《设置值》 - 为该共享页指派一个相对于其它共享页的优先级。优先级必须是介于 -1 到 9999 之间的整数，其中， -1 代表最高优先级， 9999 代表最低优先级。 如果希望确保页面在按优先级列出时能以某一特定的顺序显示，或希望确保在存在多个默认页时 （此时一个用户属于多个组）选择某一特定的页，则设置优先级的值将非常有用。
父页	如果希望该共享页成为其它共享页的子级，请单击 《选择父级》。请确保父页和子页属于**同一类别** （以防出现显示问题）。 在运行时，如果终端用户使用 《共享页导航》入口小程序，则会看到此关系。显示共享页列表时，子级将在其父级之下缩进显示。 （请注意，子页并不继承其父页的内容、自选设置或设置。反之亦然，父页在显示自己的内容时也不自动显示其子页的内容。）

属性	操作
指派类别	在以下类别中选择该页所属的类别 （可选）： ◆ 管理 ◆ 目录管理 ◆ 一般 ◆ Guest 页 ◆ 信息管理 ◆ 口令管理 如果希望确保合理组织按类别列出的页，或希望确保在对页按类别过滤后能得到适当的子集，则指派类别将非常有用。 **注释：**《Guest 页》是一种特殊的类别，用于标识可以在用户登录前 （而不是用户登录后）显示的共享页。有关更多信息，请参见第 15 章 "关于入口小程序" 在第 217 页 中有关 《共享页导航》入口小程序的部分。
说明	键入描述页的文本。

4 单击 《保存页》（位于页属性部分的底部）。

要通过复制现有页创建共享页，请执行以下操作：

1 在 《页管理》页上，选择 《维护共享页》。

将显示 《维护共享页》面板 （如上一步中所示）。

2 在共享页列表中，选择要复制的页。

提示：如果该列表较长，则可以 （按类别或起始文本）简化该列表，以便更轻易地找到所需的页。

3 选择 《复制》页操作 （位于面板左下部）。

将创建一个名为 *OriginalPageName* 拷贝的共享页。

4 指定共享页的页属性 （按上一步中说明的方法）。

5 单击 《保存页》（位于页属性部分的底部）。

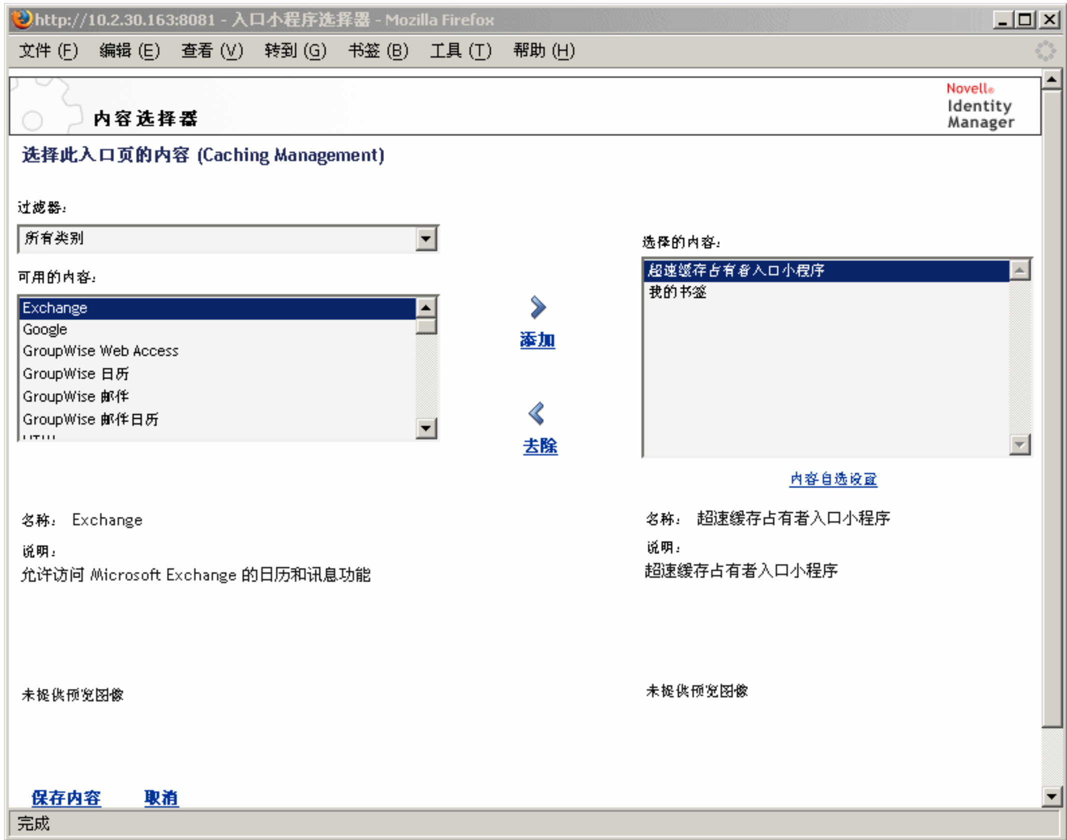
7.3.2 向共享页添加内容

创建共享页后，下一步便是选择要放置到页中的入口小程序，以此来添加内容。可以使用 Identity Manager 用户应用程序附带的预生成入口小程序，也可以使用已经注册的其它入口小程序。

要向共享页添加内容，请执行以下操作：

1 在 《维护共享页》面板中打开一个新页或现有页，然后单击 《选择内容》页任务 （位于面板底部）。

将在新的浏览器窗口中显示 《内容选择器》：



2 如果要显示特定类别的可用内容，请从 《过滤器》下拉菜单中选择类别。

3 从 《可用的内容》列表中选择一个或多个入口小程序。

提示：按住 *Ctrl* 键可从列表中选择多个不相邻的入口小程序；按住 *Shift* 键可选择多个相邻的入口小程序。

---

4 单击 《添加》将所选内容移动到 《选择的内容》列表中。

5 可以单击 《内容自选设置》来编辑为共享页选择的任何入口小程序的自选设置。指定的自选设置值将应用于显示在页中的入口小程序实例。

6 单击 《保存内容》。

现在，已经为共享页选择了内容，接下来，可以按照 "修改共享页的布局"在第 146 页 中描述的方法选择一个新布局，或按照 "排列共享页中的内容"在第 147 页 中描述的方法排列当前布局中的内容。

7.3.3 删除共享页中的内容

在创建共享页的过程中，可能需要去除页中的入口小程序从而删除内容。可以使用 《内容选择器》或 《布局选择器》，现将具体过程介绍如下。

要使用 《内容选择器》删除共享页中的内容，请执行以下操作：

1 在 《维护共享页》面板中打开一个页，然后单击 《选择内容》页任务 （位于面板底部）。

   将在新的浏览器窗口中显示 《内容选择器》（如上一步中所示）。

2 选择要从 《选择的内容》列表中删除的入口小程序，然后单击 《去除》。

   该入口小程序即从页中去除。

3 单击 《保存内容》。

要使用 《布局选择器》删除共享页中的内容，请执行以下操作：

1 在 《维护共享页》面板中打开一个页，然后单击 《排列内容》页任务 （位于面板底部）。

   将在新的浏览器窗口中显示 《布局选择器》，其中将列出该页中的入口小程序：



2 单击要去除的入口小程序的 *X* 按钮。

3 收到确认提示时，请单击 《确定》。

该入口小程序即从页中去除。

4 单击 《保存布局》。

7.3.4 修改共享页的布局

修改共享页的布局时，现有内容也将调整，以适应新的布局。某些情况下，可能需要对最终结果进行微调。

要修改共享页的布局，请执行以下操作：

1 在 《维护共享页》面板中打开一个页，然后单击 《选择布局》页任务 （位于面板底部）。

将在新的浏览器窗口中显示 《入口布局》列表：



2 通过滚动 浏览选项，并选择所需的布局。

3 单击 《选择布局》。

7.3.5 排列共享页中的内容

为共享页指定内容和布局之后，便可以将内容置于选定的布局之中，也可在特定位置添加或删除入口小程序。

要排列共享页中的内容，请执行以下操作：

1 在 《维护共享页》面板中打开一个页，然后单击 《排列内容》页任务 （位于面板底部）。

将在新的浏览器窗口中显示 《布局选择器》，其中将列出该页中的入口小程序：



2 如果要向页中添加入口小程序，请按照下列步骤操作：

2a 在所需的布局框架中单击 《添加内容》。

将在新的浏览器窗口中显示 《入口小程序选择器》。

2b 如果要显示特定类别的可用内容，请从 《过滤器》下拉菜单中选择类别。

2c 从 《可用的内容》列表中选择所需的入口小程序。

2d 单击 《选择内容》。

将关闭 《入口选择器》，并且所选择的入口小程序将显示在 《布局选择器》的目标布局框架中。

3 如果要将入口小程序移动 到布局中的其它位置，请按照下列特定于浏览器的步骤进行操作：

浏览器	操作
Internet Explorer	1. 将光标移到入口小程序的标题栏上，直到光标变为手形。 2. 按住鼠标左键，将入口小程序拖到布局中的所需位置。
Mozilla	1. 单击要移动的入口小程序。 2. 在目标布局框架内单击。 入口小程序随即会移动到目标位置。

4 如果要从布局中去除入口小程序，请按照下列步骤操作：

4a 单击要去除的入口小程序的 *X* 按钮。

4b 收到确认提示时，请单击 《确定》。

入口小程序将从布局中去除。

5 如果要编辑入口小程序的自选设置，请按照下列步骤操作：

5a 单击要编辑的入口小程序的铅笔形按钮。

浏览器中将显示入口小程序的 《内容自选设置》。

5b 根据需要更改 自选设置的值。

指定的自选设置值将应用于显示在页中的入口小程序实例。

5c 单击 《保存自选设置》。

6 单击 《保存布局》记录更改，然后关闭 《布局选择器》。

7.3.6 显示共享页

在浏览器中转到共享页的 URL 可以显示该页。

要显示共享页，请执行以下操作：

- 在万维网浏览器中，转到以下 URL：

  http://*server:port*/*IDM-war-context*/portal/pg/*shared-page-name*

  例如，若要显示名为 *MySharedPage* 的共享页，应转到：

  http://myappserver:8080/IDM/portal/pg/MySharedPage

7.4 指派页的许可权限

可以向其他用户、组和树枝指派许可权限，以使其可以使用特定的树枝页和共享页。可以指派两种安全性级别的许可权限：

许可权限	说明	可以指派的对象
查看	允许用户、组或树枝访问该页并在可用页的列表中看到该页	树枝页和共享页
所有权	允许用户、组或树枝修改页面的内容和布局，并可以将查看和所有权许可权限指派给其他用户、组和树枝	共享页

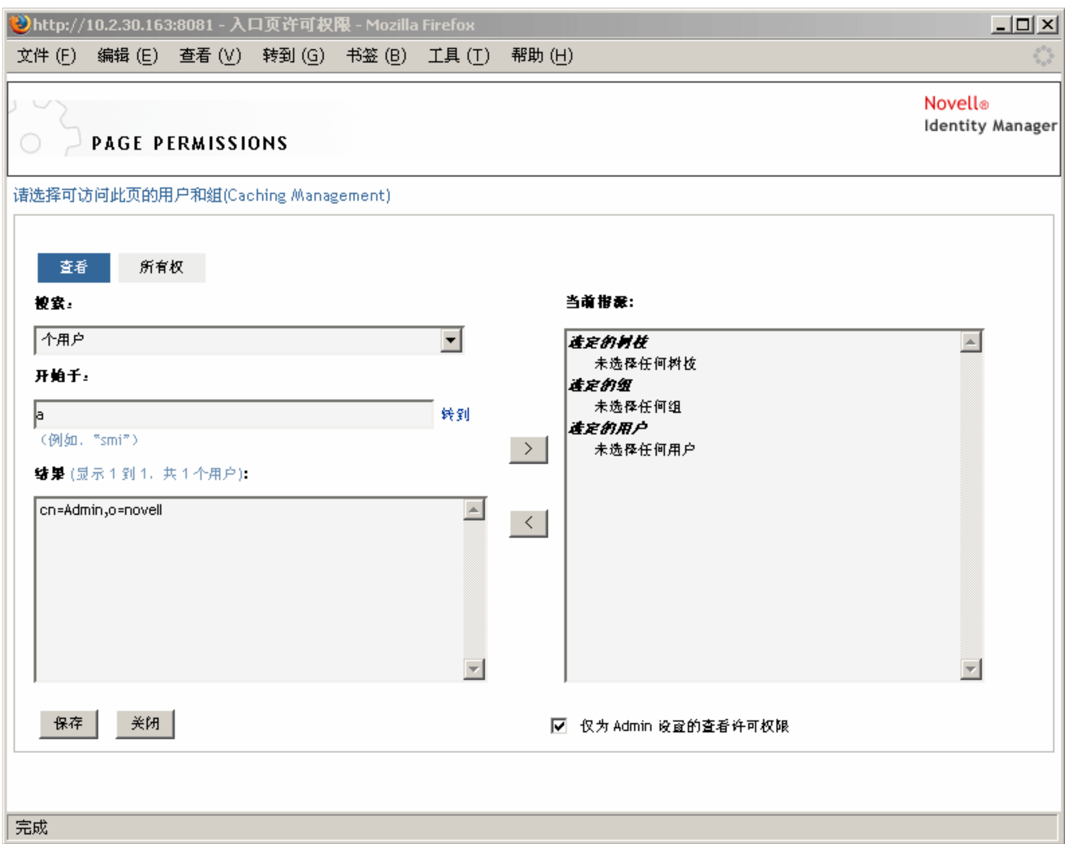
7.4.1 指派页查看许可权限

向用户指派树枝页或共享页的查看许可权限后，用户可以访问这些页，并可以在可用页列表中看到它们。

要指派树枝页或共享页的查看许可权限，请执行以下操作：

1 在 《维护树枝页》或 《维护共享页》面板中打开一个页，然后单击 《指派许可权限》页任务 （位于面板底部）。

将在新的浏览器窗口中显示 《页许可权限》对话框：



2 转至 《查看》选项卡。

3 指定以下搜索设置的值：

设置	操作
搜索主题	从下拉菜单中选择以下项之一： ◆ 用户 ◆ 组 ◆ 树枝

开始于	如果要：
	◆ 查找指定类型 （用户、组或树枝）的**所有**可用对象，请将此处设置为空白。
	◆ 查找这些对象的**子集**，请输入所需的 CN 值的起始字符。 （不区分大小写，不支持通配符。）
	例如，搜索以 S 开头的组将缩小搜索范围，并得到类似以下内容的结果：
	`cn=Sales,ou=groups,o=MyOrg`
	`cn=Service,ou=groups,o=MyOrg`
	`cn=Shipping,ou=groups,o=MyOrg`
	搜索以 Se 开头的组将返回：
	`cn=Service,ou=groups,o=MyOrg`

4 单击 《搜索》。

将在 《结果》列表中显示搜索结果。

5 选择要指派给页的用户、组或树枝，然后单击添加 (>) 按钮。

提示 **:** 按住 *Ctrl* 键可选择多项。

---

6 按照以下说明启用或禁用页面锁定功能：

如果要	操作
锁定页面后，只有用户应用程序管理员才能查看该页	选中 《仅为 Admin 设置的查看许可权限》

如果要	操作
允许所有指派的用户、组和树枝查看页	取消选中 《仅为 Admin 设置的查看许可权限》 注释：如果取消选中此设置，但没有将用户、组或树枝显式指派给该页，则所有人都将对该页拥有查看许可权限。

7 单击 《保存》，再单击 《关闭》。

7.4.2 指派共享页的拥有者

拥有共享页的用户可以修改他们所拥有的页的内容，还可以更改这些页中入口小程序的自选设置。

要指派共享页的所有权许可权限，请执行以下操作：

1 在 《维护共享页》面板打开一个页，然后单击 《指派许可权限》页任务 （位于面板底部）。

将在新的浏览器窗口中显示 《页许可权限》对话框 （如上一步中所示）。

2 转至 《所有权》选项卡。

3 指定以下搜索设置的值：

设置	操作
搜索主题	从下拉菜单中选择以下项之一： ◆ 用户 ◆ 组 ◆ 树枝

设置	操作

开始于	如果要：
	◆ 查找指定类型 （用户、组或树枝）的**所有**可用对象，请将此处设置为空白。
	◆ 查找这些对象的**子集**，请输入所需的 CN 值的起始字符。 （不区分大小写，不支持通配符。）
	例如，搜索以 S 开头的组将缩小搜索范围，并得到类似以下内容的结果：
	`cn=Sales,ou=groups,o=MyOrg`
	`cn=Service,ou=groups,o=MyOrg`
	`cn=Shipping,ou=groups,o=MyOrg`
	搜索以 Se 开头的组将返回：
	`cn=Service,ou=groups,o=MyOrg`

4 单击 《搜索》。

将在 《结果》列表中显示搜索结果。

5 选择要指派给页的用户、组或树枝，然后单击添加 (>) 按钮。

提示 **:** 按住 *Ctrl* 键可选择多项。

6 按照以下说明启用或禁用页面锁定功能：

如果要	操作
锁定页面后，只有用户应用程序管理员才能使用该页	选中 《仅为 Admin 设置的所有权许可权限》
允许所有指派的用户、组和树枝使用页	取消选中 《仅为 Admin 设置的所有权许可权限》 注释 **:** 如果取消选中此设置，但没有将用户、组或树枝显式指派给该页，则**所有人都将对该页拥有所有权许可权限**。

7 单击 《保存》，再单击 《关闭》。

7.4.3 启用用户对 《创建用户或组》页的访问权限

默认情况下，只有用户应用程序管理员才可以查看和使用 《创建用户或组》页。该共享页位于 Identity Manager 用户界面的 《身份自助服务》选项卡上。但是在适当的情况下，用户应用程序管理员也可以将许可权限指派给一个或多个终端用户，以便他们也能访问该页。例如，选定的处于管理层的人员可能需要拥有自己创建用户、组或任务组的能力。

要向用户授予 《创建用户或组》页的访问权限，请执行以下操作：

1 在 《维护共享页》面板中，打开名为 《创建用户或组》的页。

2 使用 《指派许可权限》页任务，将查看许可权限授予 《创建用户或组》共享页的适当用户、组或树枝。

3 从 《页管理》切换到 《入口小程序管理》，然后打开名为 *CreatePortlet* 的入口小程序注册 （在 《创建用户或组》页上使用）。

4 使用 《安全性》面板将列出和执行许可权限授予 CreatePortlet 入口小程序注册的适当用户、组或树枝。

   有关指派入口小程序的许可权限的更多信息，请参见第 9 章 “入口小程序管理”在第 165 页 。

5 转至 *iManager*，然后使用管理员帐户登录到 *Identity Vault* 的树中。

6 请确保将使用 《创建用户或组》的人员对要在其中创建对象 （用户、组或任务组）的树枝拥有创建 *[Entry Rights]* 属性的权限。

   例如，可以修改选定树枝的受托者，并将适当的用户、组或树枝添加为受托者。然后，可以将以下权限指派给每位受托者：

属性名	指派的权限	继承
[All Attributes Rights]	◆ 比较 ◆ 读 ◆ 写	是 （选中此复选框）
[Entry Rights]	◆ 浏览 ◆ 创建	是 （选中此复选框）

   如果未指派 Identity Vault 中的必需权限 （或由于某种原因无法派生那些权限），终端用户可能会收到一条错误讯息，例如下面这条来自 《创建用户或组》的错误讯息：

```
User 'cn=mmackenzie,ou=users,ou=idmsample,o=novell' does not have
permission to create
'cn=MyNewGroup,ou=groups,ou=idmsample,o=novell' or modify related
objects.
```

若要了解 （具有访问权限的用户）如何使用 《创建用户或组》，请参见 《*Identity Manager* 用户应用程序：用户指南》。

7.4.4 启用用户对各个管理页的访问权限

默认情况下，只有用户应用程序管理员才能访问 Identity Manager 用户界面的 《管理》选项卡以及该选项卡中包含的各个页 （《页管理》、《主题》、《入口小程序管理》、《入口》、《安全性》、《日志记录》、《超速缓存》、《工具》）。但如果需要的话，用户应用程序管理员可以将许可权限指派给一个或多个终端用户，以便他们能查看和使用 《管理》选项卡上的特定页。例如，一个小组的用户可能需要定期更改主题，虽然他们不是用户应用程序管理员。

要向用户授予各个管理页的访问权限，请执行以下操作：

1 在 《维护树枝页》面板中打开 《管理树枝页》。

   这是转至 Identity Manager 用户界面的 《管理》选项卡时所使用的树枝页。

2 使用 《指派许可权限》页任务，将查看许可权限授予 《管理树枝页》的适当用户、组或树枝。

3 在 《维护共享页》面板中，打开适当的管理页 （《管理》类别下的一个共享页）。

4 使用 《指派许可权限》页任务，将查看和所有权许可权限授予该共享页的适当用户、组或树枝。

5 请确保指定的用户、组或树枝对指定页中使用的每个入口小程序都拥有执行许可权限（如果已经限制了那些入口小程序）。

   有关指派入口小程序的许可权限的更多信息，请参见第 9 章 “入口小程序管理”在第 165 页 。

7.5 设置组的默认页

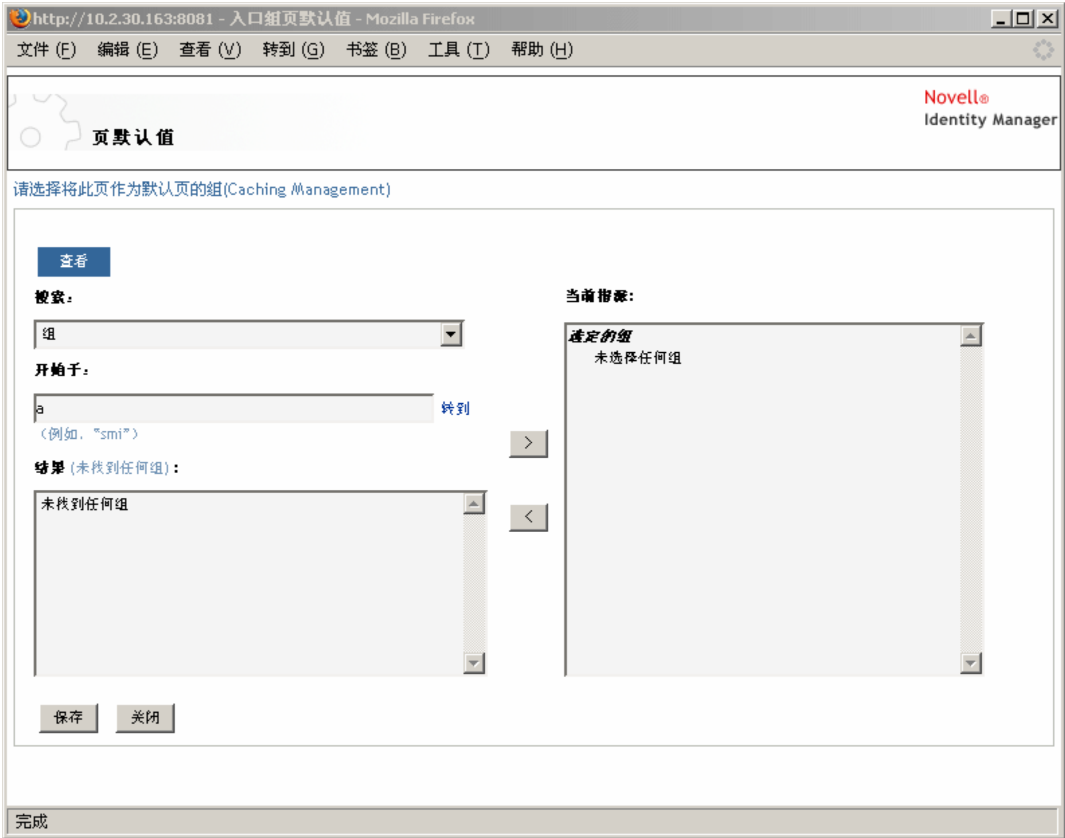
可以向任何已授权的用户组指派一个默认树枝页和一个默认共享页。这些设置将影响用户登录时看到的树枝页以及他们在树枝页上看到的共享页。

如果用户属于多个具有默认页指派的组，则将使用导航优先级确定要显示的树枝页和共享页。

要向组指派默认树枝页或默认共享页，请执行以下操作：

1 在 《维护树枝页》或 《维护共享页》面板上打开一个页，然后单击 《设置为默认值》页任务 （位于面板底部）。

将在新的浏览器窗口中显示 《页默认值》对话框：



2 指定以下搜索设置的值：

设置	操作
搜索主题	(（已自动选择了 《组》。）

设置	操作

开始于	如果要：
	◆ **查找所有**可用组，请将此处设置为空白。
	◆ **查找这些组的子集**，请输入所需的 CN 值的起始字符。（不区分大小写，不支持通配符。）
	例如，搜索以 S 开头的组将缩小搜索范围，并得到类似以下内容的结果：
	`cn=Sales,ou=groups,o=MyOrg`
	`cn=Service,ou=groups,o=MyOrg`
	`cn=Shipping,ou=groups,o=MyOrg`
	搜索以 Se 开头的组将返回：
	`cn=Service,ou=groups,o=MyOrg`

3 单击 《搜索》。

将在 《结果》列表中显示搜索结果。

4 选择要将此页作为其默认页的组，然后单击添加 (>) 按钮。

提示 **:** 按住 *Ctrl* 键可选择多项。

---

5 单击 《保存》，再单击 《关闭》。

7.6 为树枝页选择默认共享页

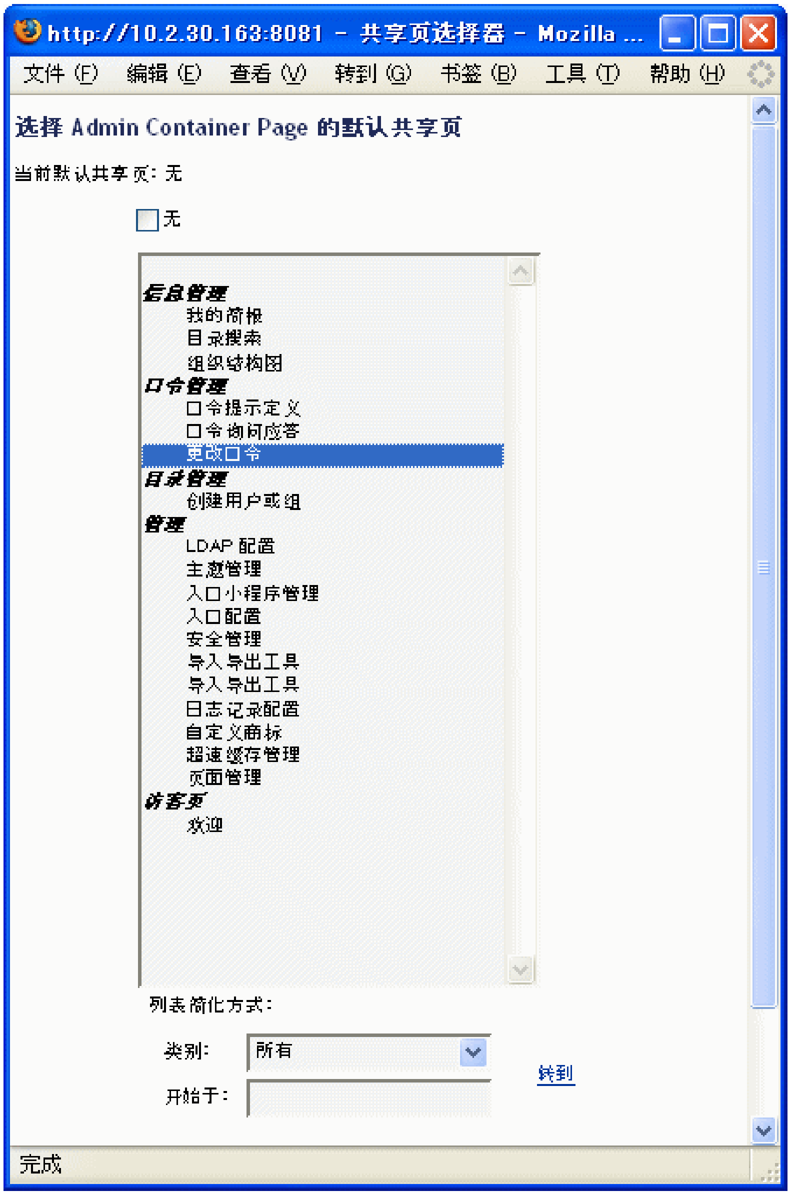
可以向所拥有的每个树枝页指派一个默认共享页。用户界面在确定显示内容时将考虑此页指派。

要为树枝页指派默认共享页，请执行以下操作：

1 在 《维护树枝页》面板上打开一个树枝页。

2 在页属性部分，查找 《默认共享页》并单击 《选择默认值》。

将在新的浏览器窗口中显示 《选择默认共享页》对话框：



3 如果共享页的列表较长，可以 （通过类别或起始文本）简化该列表，从而更轻松地找到所需的页。
4 选择一个共享页以用作树枝页的默认页 （或选中 《无》以不设置默认页）。
5 单击 《保存》以接受选择并关闭对话框。
6 单击 《保存页》（位于页属性部分的底部）。

主题配置

8

本章将说明如何使用 Identity Manager 用户界面上 《管理》选项卡的 《主题》页。包括以下主题：

有关访问和使用 《管理》选项卡的更多一般信息，请参见第 6 章 “使用 《管理》选项卡”在第 119 页 。

8.1 关于主题配置

使用 《主题》页可以控制 Identity Manager 用户界面的外观。

主题是应用于整个用户界面的一组视觉特征 （包括来宾和登录页、《身份自助服务》选项卡、《请求和批准》选项卡和 《管理》选项卡）。用户界面始终都仅存在一个有效主题。《主题》页提供多个主题选项，以便在不同主题间进行切换。

在 《主题》页中，还可以：

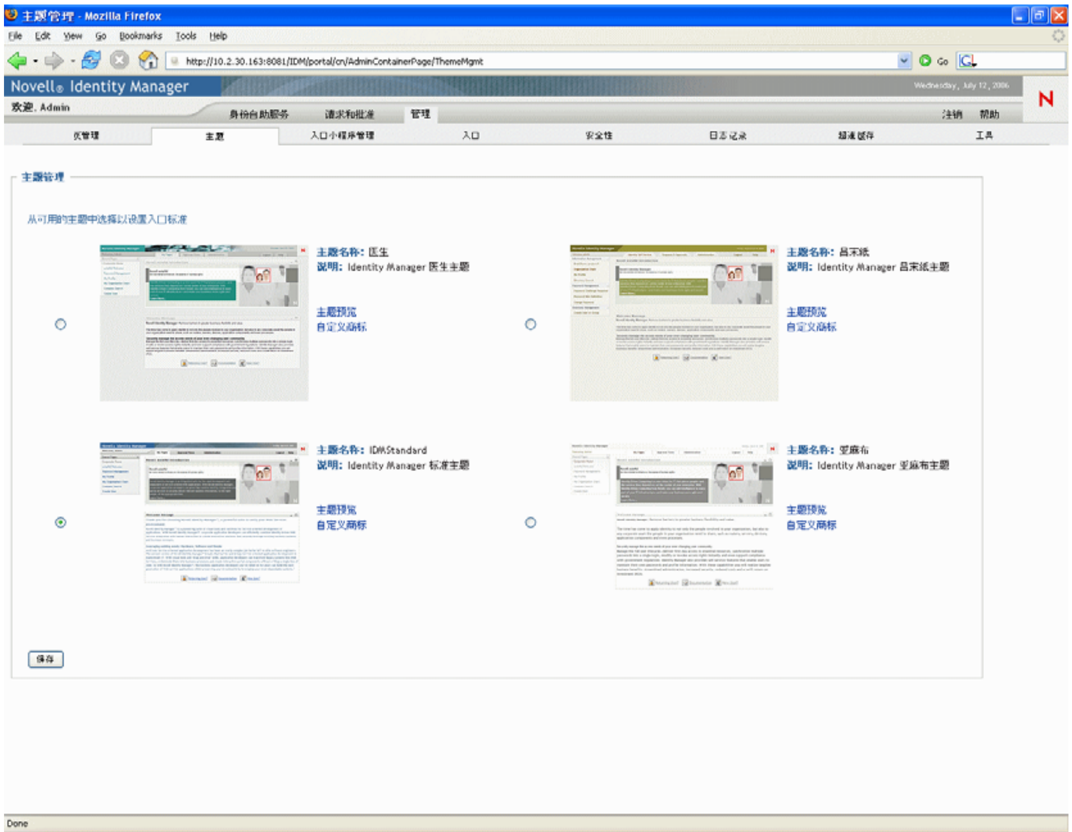
- 预览每个主题选项，以查看其外观
- 自定义任意主题选项，以反映您的商标 （图徽等）

8.2 预览主题

在选择主题之前，可以对主题进行预览，查看它将如何更改 Identity Manager 用户界面的外观。

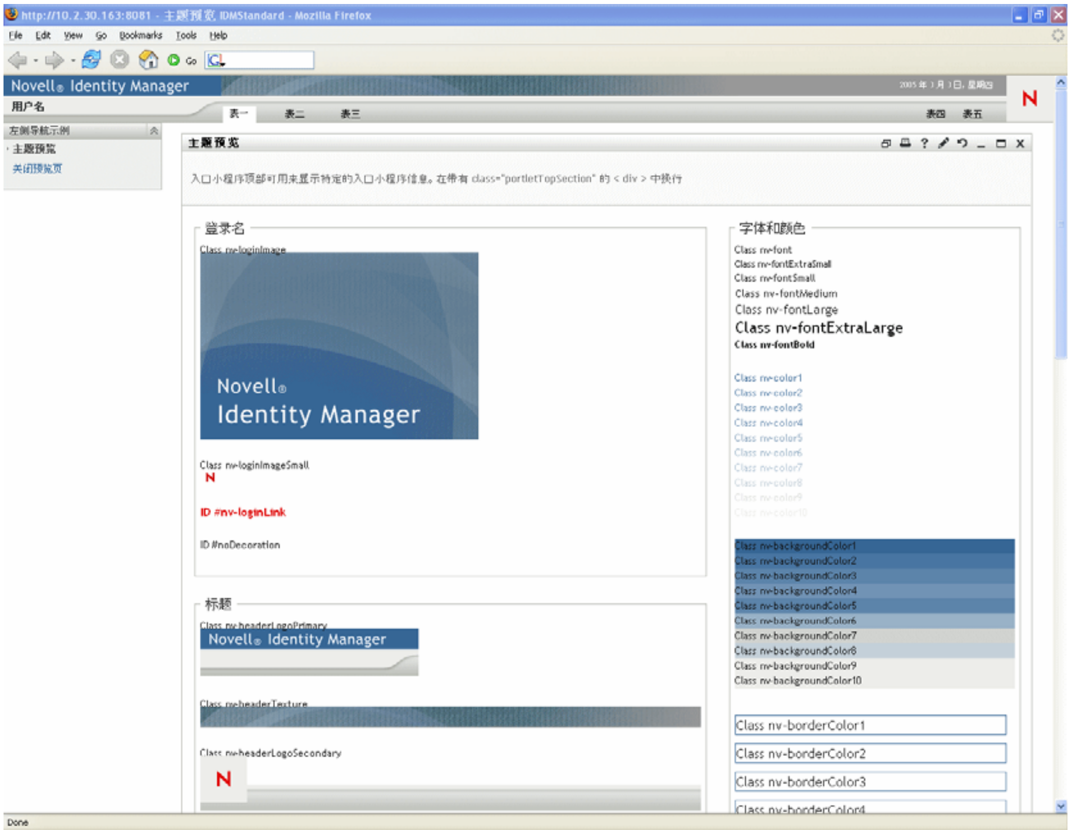
要预览主题，请执行以下操作：

1 转至 《主题》页：



2 找到一个自己感兴趣的主题，然后单击相应的 《主题预览》链接。

将在新的浏览器窗口中显示该主题的预览：



3 通过滚动进行预览，查看该主题的特征。

4 查看完毕后，请单击 《关闭预览页》（位于左上角）或手工关闭预览窗口。

8.3 选择主题

找到喜欢的主题后，可以选择将其设置为 Identity Manager 用户界面的当前主题。

要选择主题，请执行以下操作：

1 转至 《主题》页。

2 单击所需主题的单项选择按钮。

3 单击 《保存》按钮。

用户界面的外观将更改，以反映所选择的主题。

8.4 自定义主题的商标

可以通过替换为自己的图像并更改某些颜色设置来调整所有的主题。通过这一方式，可以自定义 Identity Manager 用户界面的外观，使其更加符合贵公司或组织的商标要求。

要自定义主题的商标，请执行以下操作：

1 转至 《主题》页。

2 找到要进行调整的主题，然后单击相应的 《自定义商标》链接。

《主题》页将显示该主题的 《自定义商标》设置：





3 根据需要在这些设置中指定自定义设置，其中包括：

- 标题图像
- 导航区域颜色
- 登录图像

按照屏幕上的说明指定每项设置。

4 单击 《保存》按钮。

如果正在编辑当前主题，用户界面的外观将随之更改，以反映自定义设置。 （如果希望复原对主题所做的自定义设置，请单击 《重设置》）。

注释 :《主题预览》按钮在自定义期间可用，但请注意，它总是显示主题的原始特征，而不会显示所做的更改。

---

5 对此主题修改完毕后，请单击 《返回到主题选择器》按钮。

入口小程序管理

9

本章将说明如何使用 Identity Manager 用户界面上 《管理》选项卡的 《入口小程序管理》页。包括以下主题：

- "关于入口小程序管理"在第 165 页
- "管理入口小程序应用程序"在第 165 页
- "管理入口小程序定义"在第 168 页
- "管理已注册的入口小程序"在第 172 页

有关访问和使用 《管理》选项卡的更多一般信息，请参见第 6 章 "使用 《管理》选项卡"在第 119 页 。

9.1 关于入口小程序管理

使用 《入口小程序管理》页，可以控制 Identity Manager 用户界面上可用的入口小程序以及有权访问它们的用户。入口小程序是可插入的用户界面要素 （基于 *Java* 标准），用于向用户界面中的页 （包括树枝页和共享页）提供内容。

管理小程序需要处理以下内容：

处理的内容	说明
入口小程序应用程序	与 Java Portlet 1.0 兼容的 WAR，其中包含入口小程序部署描述符 portlet.xml 以及其它可选的入口小程序运行时工件。 请参见 "管理入口小程序应用程序"在第 165 页 。
入口小程序定义	用于指定入口小程序配置参数的描述符 （读取自 portlet.xml）。应用程序中的每个入口小程序均有一个定义。 请参见 "管理入口小程序定义"在第 168 页 。
入口小程序注册	基于入口小程序定义的入口小程序注册。一个入口小程序应用程序中可以有同一入口小程序的多个注册。 请参见 "管理已注册的入口小程序"在第 172 页 。

有关 Identity Manager 用户界面附带的入口小程序的详情，请参见 "入口小程序参照"在第 215 页 。若要了解如何在树枝页和共享页上使用入口小程序，请参见第 7 章 "页管理"在第 125 页 。

9.2 管理入口小程序应用程序

安装 Identity Manager 用户应用程序后，会将 *IDM.war* 部署到应用程序服务器中，并自动注册为入口小程序应用程序。IDM.war （可在安装时重命名）包括 Identity Manager 用户界面的默认配置中使用的所有入口小程序。此外，它还包括默认情况下不会使用的一些附加入口小程序。 （有关 IDM.war 入口小程序的详情，请参见 "入口小程序参照"在第 215 页 。）

但除了使用 IDM.war 入口小程序以外，还可以使用其它入口小程序。如果将任何其它标准入口小程序应用程序 （与 Java Portlet 1.0 兼容的 WAR）部署到应用程序服务器上，就可以

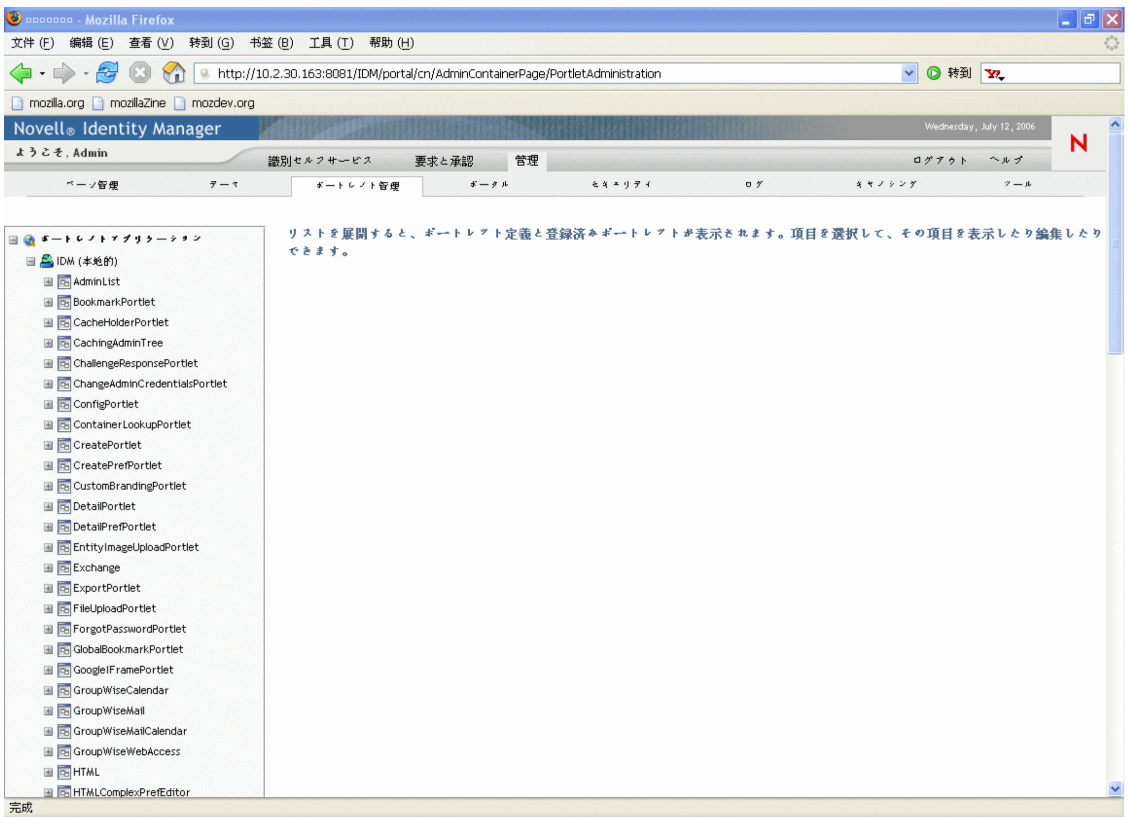
使用这些入口小程序应用程序及其在 Identity Manager 用户界面中的入口小程序。例如，可以看到这些入口小程序应用程序与 IDM.war 同时列于 《入口小程序管理》页中。

在 《入口小程序管理》页中，可以通过以下方式管理 *IDM.war* 及其它入口小程序应用程序：

- “访问服务器上的入口小程序应用程序”在第 166 页
- “查看有关入口小程序应用程序的信息”在第 166 页
- “取消注册入口小程序应用程序”在第 167 页

9.2.1 访问服务器上的入口小程序应用程序

转至 《入口小程序管理》页时，它将自动显示一个列表，其中将列出部署在应用程序服务器上的入口小程序应用程序 （IDM.war 及其它）。该列表将以树的形式显示在左侧，可以在其中执行展开和导航操作，以管理所选的入口小程序应用程序及其内容：



9.2.2 查看有关入口小程序应用程序的信息

可以查看以下有关已列出入口小程序应用程序的只读信息：

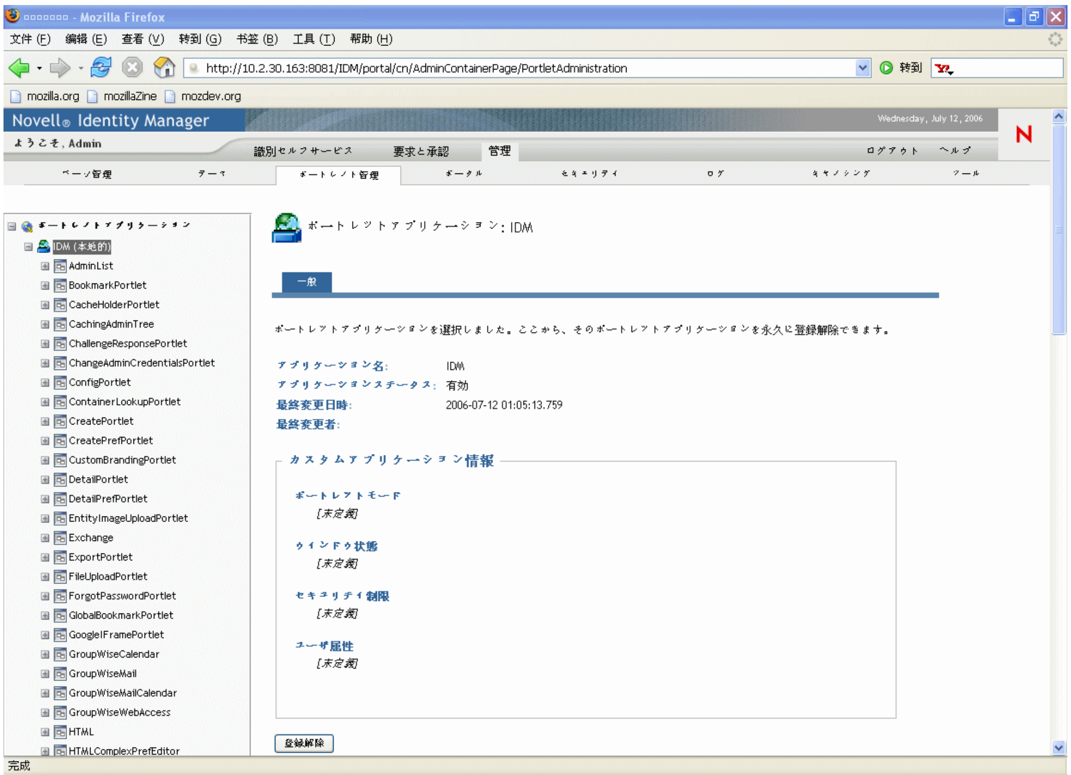
- 名称
- 状态 （启用或禁用）
- 上次修改日期
- 上次修改应用程序的用户

- 自定义应用程序信息 （如果有）：入口小程序方式、窗口状态、安全约束和用户特性

要查看有关入口小程序应用程序的信息，请执行以下操作：

- 在 《入口小程序应用程序》列表中，选择要了解的入口小程序应用程序。

  右侧将显示 《一般》面板，其中将列出所选入口小程序应用程序的信息：



9.2.3 取消注册入口小程序应用程序

如果希望将入口小程序应用程序从应用程序服务器中去除，则在取消部署之前，必须先将它取消注册。否则，入口小程序应用程序将在重启动服务器时自动完成重新部署。

取消注册入口小程序应用程序时，所有相关的自选设置和设置都将从储存应用程序数据的数据库中去除。

注释：由于本地入口小程序树枝是入口的本地入口小程序应用程序，因此无法将其取消注册。本地入口小程序树枝管理入口 （Identity Manager 用户应用程序）中包含的入口小程序。

要取消注册入口小程序应用程序，请执行以下操作：

1 在 《入口小程序应用程序》列表中选择要取消注册的入口小程序应用程序。

将在右侧显示 《一般》面板 （如上一步中所示）。

2 单击 《取消注册》。

将显示一个确认窗口。

3 单击 《确定》确认操作。

完成此过程后，取消注册的入口小程序应用程序将从 《入口小程序应用程序》列表中去除。

4 若要将入口小程序应用程序从应用程序服务器中去除，请使用服务器工具对包含该入口小程序应用程序的存档取消部署。

注释 **:** 若要重新注册一个已取消注册的入口小程序应用程序，必须先对其进行重新部署。

9.3 管理入口小程序定义

在 《入口小程序管理》页中，可以执行以下与入口小程序应用程序中的入口小程序定义相关的任务：

- "访问已部署的入口小程序应用程序中的入口小程序定义"在第 168 页
- "注册入口小程序定义"在第 169 页
- "查看有关入口小程序定义的信息"在第 170 页

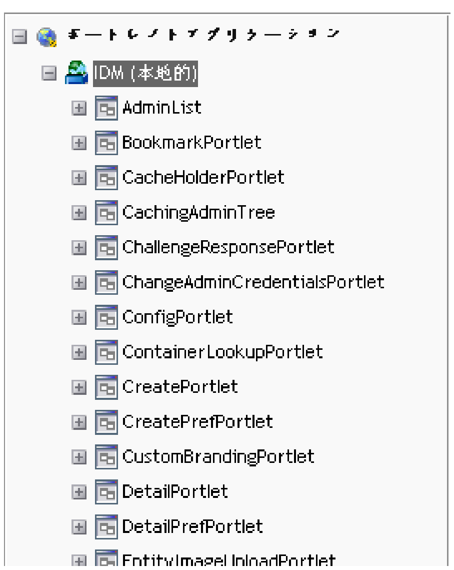
9.3.1 访问已部署的入口小程序应用程序中的入口小程序定义

《入口小程序应用程序》列表将显示所选入口小程序应用程序中的入口小程序定义。

要访问已部署的入口小程序应用程序中的入口小程序定义，请执行以下操作：

- 在 《入口小程序应用程序》列表中，展开要访问其入口小程序定义的入口小程序应用程序。

  该树将显示该入口小程序应用程序下的所有入口小程序定义：



9.3.2 注册入口小程序定义

在使用入口小程序之前，必须使用入口 （Identity Manager 用户应用程序）注册其定义。已注册的入口小程序定义称为入口小程序注册。可以为一个入口小程序创建多个注册，这样就可以在同一页中放置该入口小程序的多个实例。

入口小程序注册将继承入口小程序类的所有自选设置和设置，但仍可以通过以下方式修改这些值：

- 注册入口小程序定义时 - 请参见“管理已注册的入口小程序”在第 172 页
- 向页中添加入口小程序的实例时 - 请参见第 7 章 “页管理”在第 125 页

Identity Manager 用户应用程序附带的所有入口小程序都将自动注册。

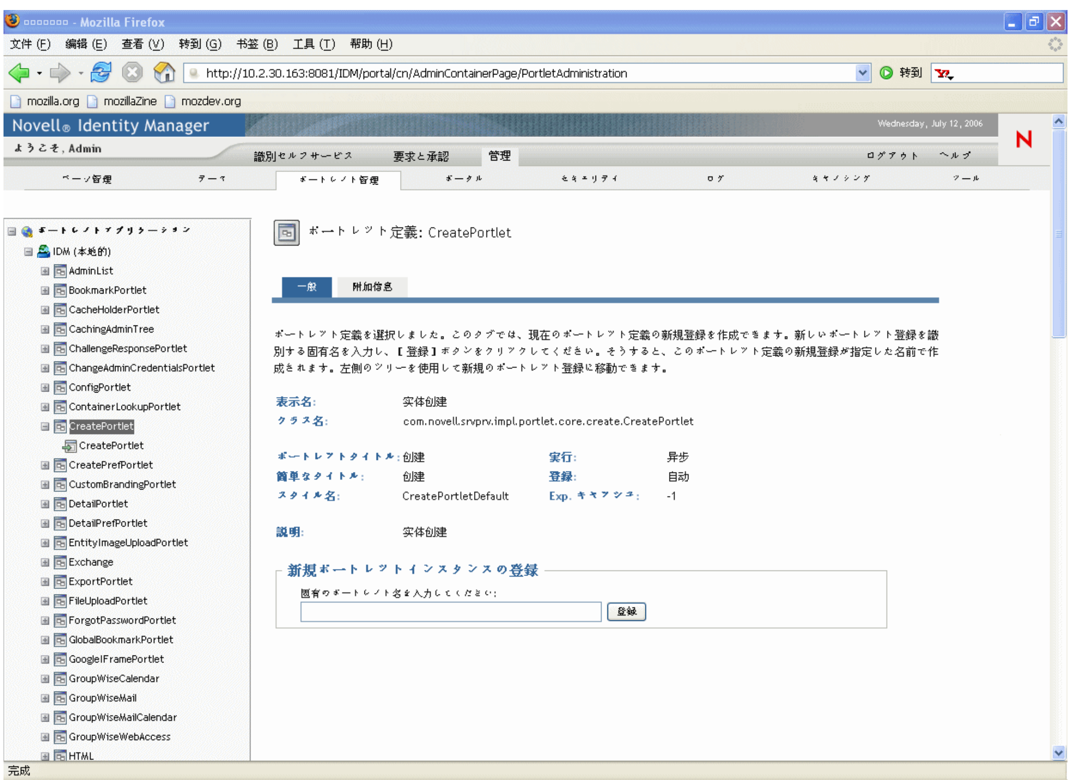
编辑方式 如果入口小程序定义提供编辑方式，则终端用户便可以根据入口小程序 doEdit() 方法的逻辑，在运行时修改入口小程序注册的特定自选设置。

Identity Manager 用户应用程序还为编辑方式提供了一个默认实施。如果未显式实施 doEdit() 方法，则将显示默认的自选设置页。

要注册入口小程序定义，请执行以下操作：

1 在 《入口小程序应用程序》列表中，选择要创建入口小程序注册的入口小程序定义。

将在右侧显示 《一般》面板：



请注意，所有选定入口小程序的现有注册都列出在 《入口小程序应用程序》树中 （位于左侧）相应的入口小程序定义名称下。

2 在 《注册新的入口小程序实例》文本框中，输入入口小程序注册的唯一名称，然后单击 《注册》。

将创建新的入口小程序注册，并将其列出在 《入口小程序应用程序》树中。

3 如果要修改新入口小程序注册的自选设置和设置，请参见"管理已注册的入口小程序"在第 172 页 。

9.3.3 查看有关入口小程序定义的信息

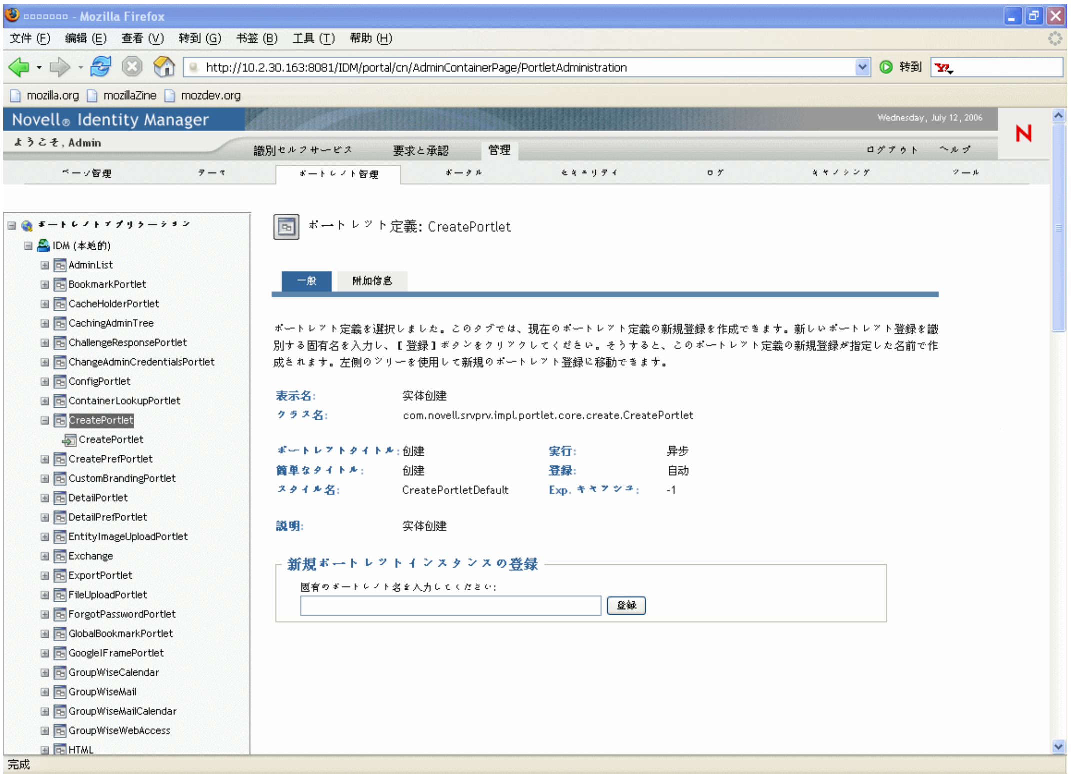
可以查看以下有关已列出的入口小程序定义的只读信息：

- 显示名称
- 类名
- 入口小程序标题
- 执行类型 （同步或异步）
- 短标题
- 注册类型
- 样式名称
- 超速缓存失效时间
- 说明
- 初始化参数
- 关键字
- 支持的 MIME 类型
- 入口小程序支持的方式
- 支持的区域设置
- 支持的设备
- 安全职能

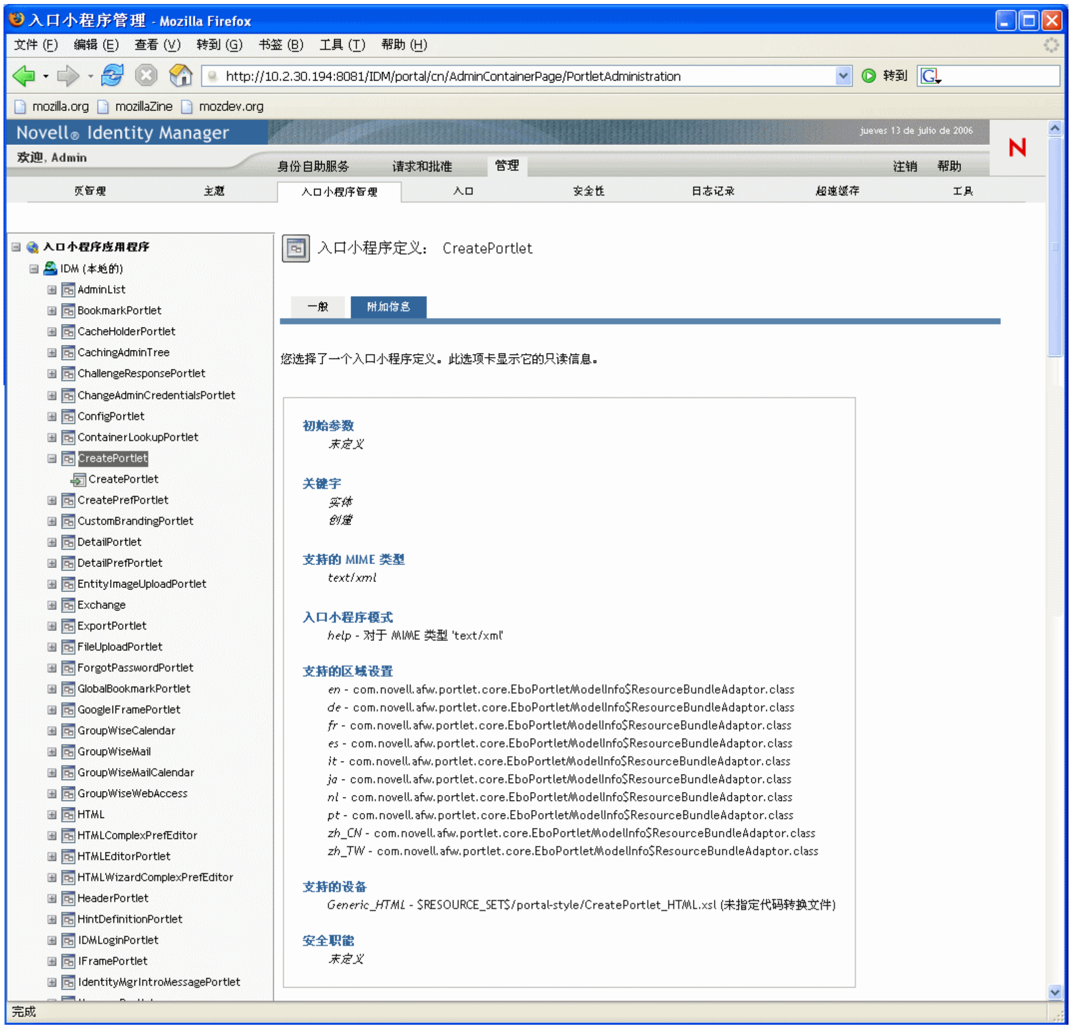
要查看有关入口小程序定义的信息，请执行以下操作：

1 在 《入口小程序应用程序》列表中，选择要了解的入口小程序定义。

将在右侧显示 《一般》面板，其中将列出有关所选入口小程序定义的信息：



2 转至 《附加信息》面板，查看所选入口小程序定义的更多细节：



9.4 管理已注册的入口小程序

在 《入口小程序管理》页中，可以执行以下与入口小程序应用程序中的入口小程序注册相关的任务：

- “在已部署的入口小程序应用程序中访问入口小程序注册” 在第 173 页
- “查看有关入口小程序注册的信息” 在第 174 页
- “向入口小程序注册指派类别” 在第 174 页
- “修改入口小程序注册的设置” 在第 175 页
- “修改入口小程序注册的自选设置” 在第 178 页
- “指派入口小程序注册的安全性许可权限” 在第 179 页

* “取消注册入口小程序”在第 182 页

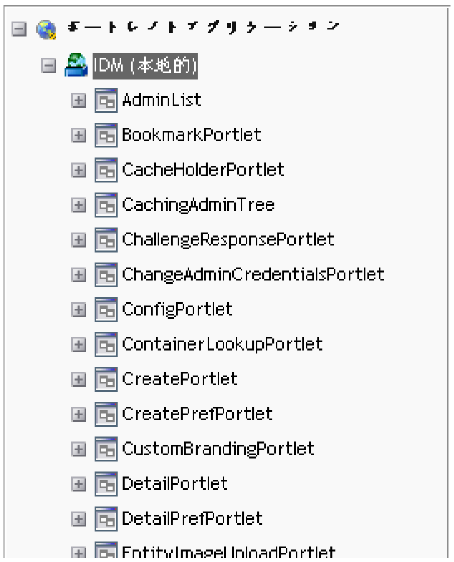
9.4.1 在已部署的入口小程序应用程序中访问入口小程序注册

《入口小程序应用程序》列表将显示所选入口小程序应用程序中每个入口小程序定义的入口小程序注册。

要访问已部署的入口小程序应用程序中的入口小程序注册，请执行以下操作：

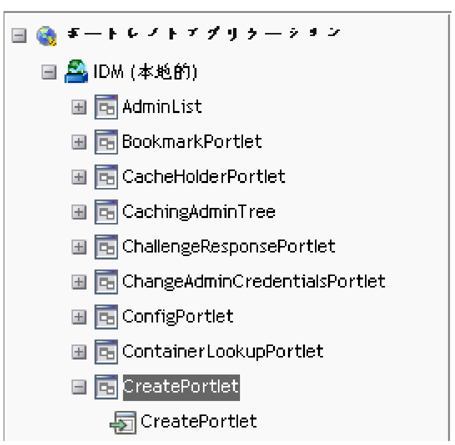
1 在 《入口小程序应用程序》列表中，请将要访问其入口小程序定义和注册的入口小程序应用程序展开。

该树将显示该入口小程序应用程序下的所有入口小程序定义：



2 对于要访问的入口小程序注册，请展开其入口小程序定义。

该树将显示该入口小程序定义下的所有入口小程序注册：



9.4.2 查看有关入口小程序注册的信息

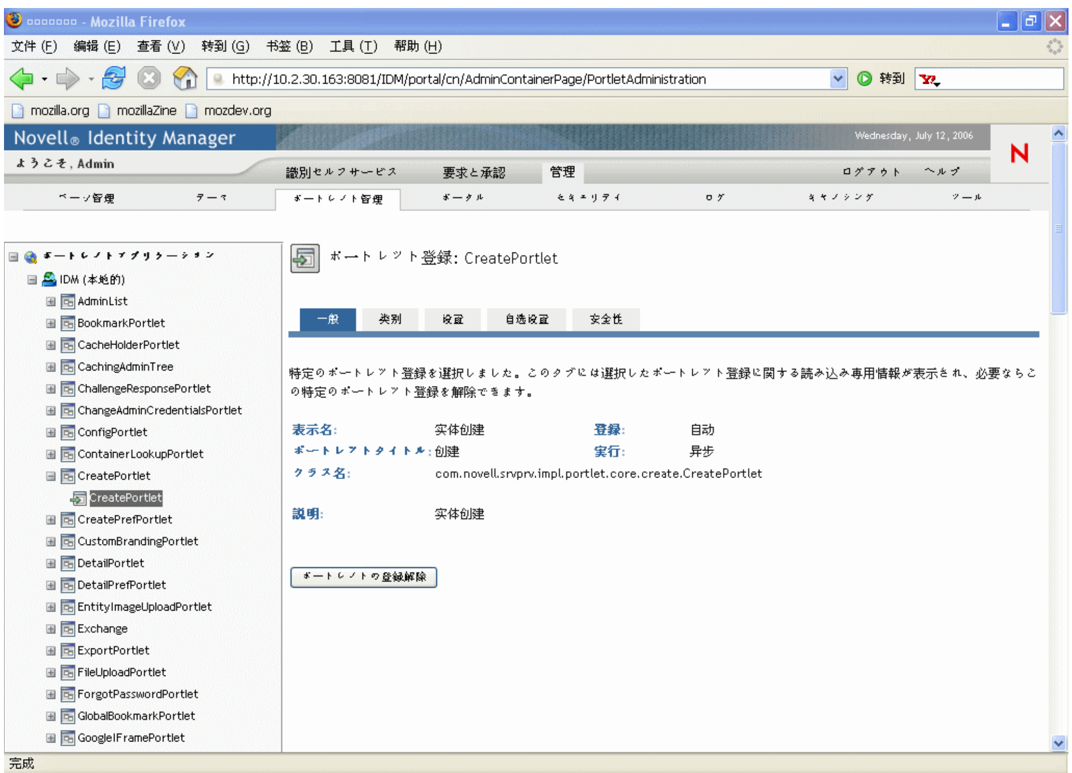
可以查看以下有关已列出的入口小程序注册的只读信息：

- 显示名称
- 注册类型
- 入口小程序标题
- 执行类型 （同步或异步）
- 类名
- 说明

要查看有关入口小程序注册的信息，请执行以下操作：

- 在 《入口小程序应用程序》列表中，选择要了解的入口小程序注册。

  将在右侧显示 《一般》面板，其中将列出有关所选入口小程序注册的信息：



9.4.3 向入口小程序注册指派类别

可以按类别组织入口小程序注册，以便在入口小程序应用程序中搜索特定的入口小程序。

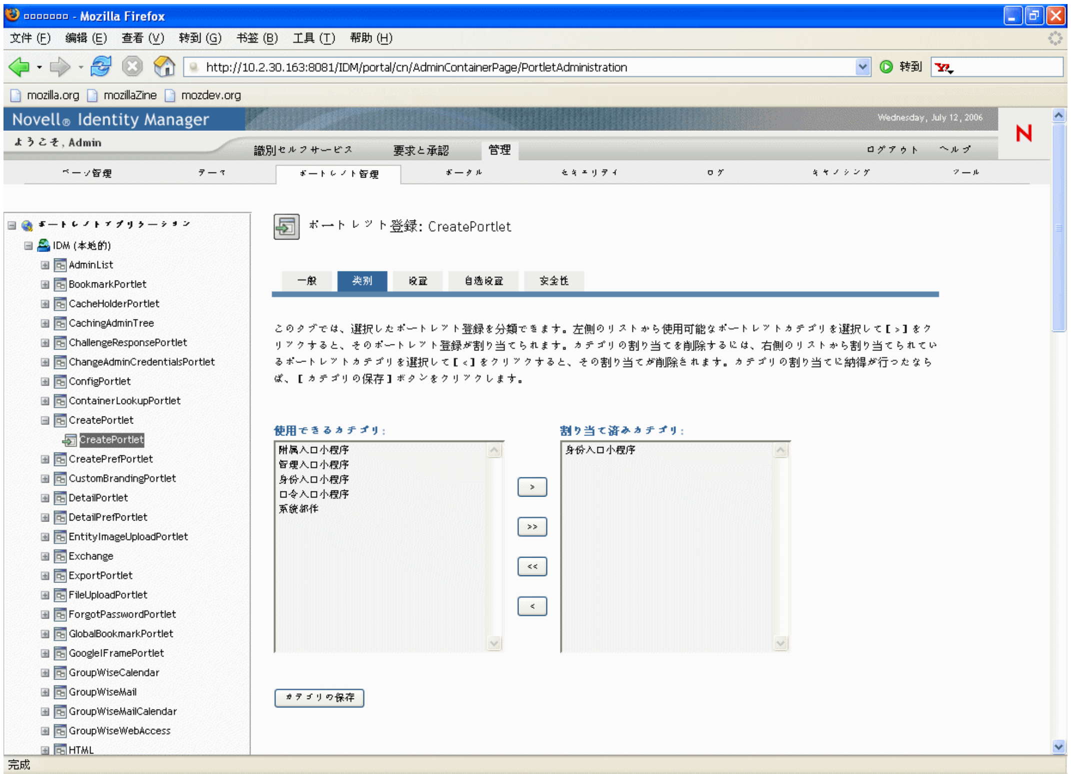
要为入口小程序注册指派类别，请执行以下操作：

1 在 《入口小程序应用程序》列表中，选择要分类的入口小程序注册。

  将在右侧显示 《一般》面板。

2 转至 《类别》面板。

该面板将显示所选入口小程序注册的已指派的可用类别列表：



3 根据需要更新 《指派的类别》列表：

如果要	操作
向入口小程序注册指派一个或多个类别	选择每个要指派的类别并单击 **>**
向入口小程序注册指派所有类别	单击 **>>**
去除一个或多个类别指派	选择每个要去除的类别，然后单击 **<**
去除所有的类别指派	单击 **<<**

4 单击 《保存类别》。

9.4.4 修改入口小程序注册的设置

入口小程序设置定义入口 （Identity Manager 用户应用程序）与各个入口小程序进行交互的方式。每个入口小程序都配置了以下设置：

- 职务
- 最大超时值
- 需要鉴定
- 显示标题栏

- 对用户隐藏
- 在入口小程序应用程序中定义的选项

标准 Java Portlet 1.0 设置在入口小程序应用程序 WAR 的入口小程序部署描述符 (portlet.xml) 中定义。在 《入口小程序管理》页中，可以逐注册更改这些设置的值。此时，新值仅对所选的入口小程序注册有效。

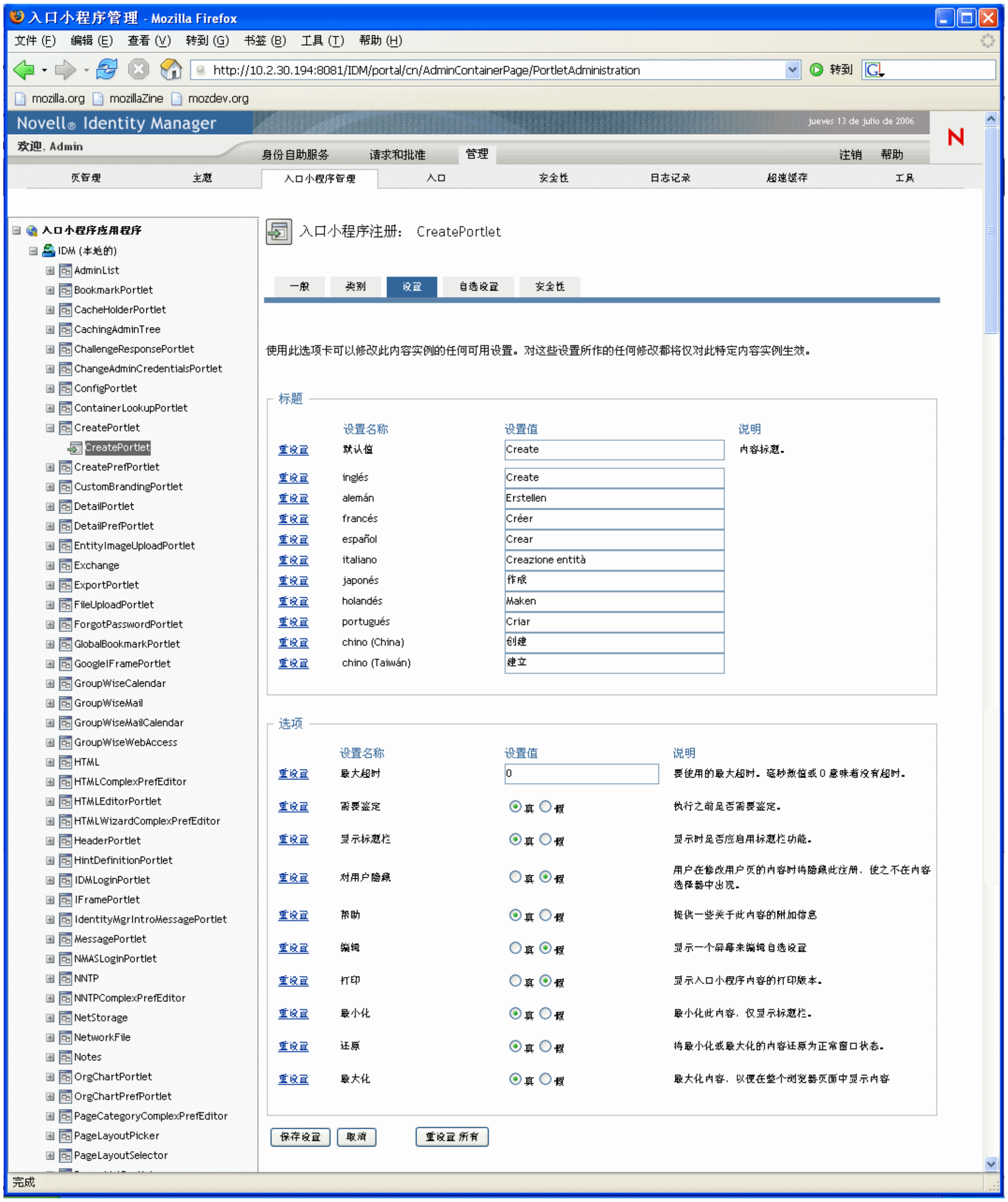
要修改入口小程序注册设置，请执行以下操作：

1 在 《入口小程序应用程序》列表中，选择要修改其设置的入口小程序注册。

   将在右侧显示 《一般》面板。

2 转至 《设置》面板。

该面板将显示所选入口小程序注册的当前设置：



3 根据需要修改设置。

请注意，在此面板中还可以执行以下操作：

如果要	操作
丢弃未保存的更改	单击 《取消》

如果要	操作
将此入口小程序注册的所有设置返回为它们的默认值（在相应的入口小程序定义中定义）	单击 《全部重设置》
将单个设置返回为其默认值	单击该设置旁的 《重设置》链接

4 单击 《保存设置》。

9.4.5 修改入口小程序注册的自选设置

入口小程序自选设置由入口小程序开发者在设计期间使用入口小程序开发描述符定义。由于入口小程序开发者实施方法不同，因此入口小程序的自选设置都各不相同。

在 《入口小程序管理》页中，可以逐注册更改这些自选设置的值。此时，新值仅对所选的入口小程序注册有效。

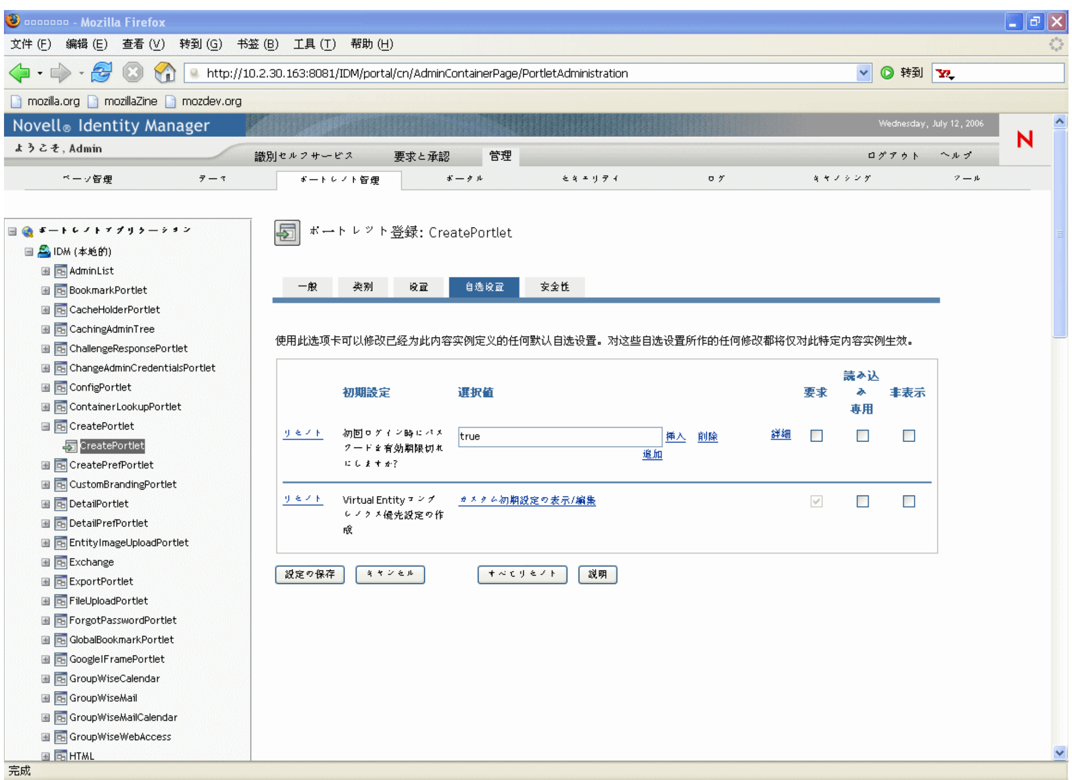
要修改入口小程序注册自选设置，请执行以下操作：

1 在 《入口小程序应用程序》列表中，选择要修改其自选设置的入口小程序注册。

将在右侧显示 《一般》面板。

2 转至 《自选设置》面板。

该面板中显示所选入口小程序注册的当前自选设置：



3 根据需要修改自选设置。

请注意，在此面板中还可以执行以下操作：

如果要	操作
显示有关自选设置的更多信息	单击 《说明》
丢弃未保存的更改	单击 《取消》
将此入口小程序注册的所有自选设置返回为它们的默认值 （在相应的入口小程序定义中定义）	单击 《全部重设置》
将单个自选设置返回为其默认值	单击该自选设置旁的 《重设置》链接

4 要修改入口小程序定义中指定的每个区域设置的本地化版本自选设置，请按照下列步骤操作：

4a 单击该自选设置旁的 《细节》链接 （如果可用）。

面板将显示每个区域设置的自选设置值。

4b 根据需要修改值。

4c 单击 《确定》，应用所做的更改并返回自选设置主列表。

5 单击 《保存自选设置》。

9.4.6 指派入口小程序注册的安全性许可权限

可以将以下安全性许可权限指派给用户、组和树枝，以进行入口小程序注册：

许可权限	说明
列表	用户可以从选择列表中**查看**入口小程序注册
执行	用户可以在入口页**运行**入口小程序注册

修改安全性许可权限时，新值仅对所选的入口小程序注册有效。

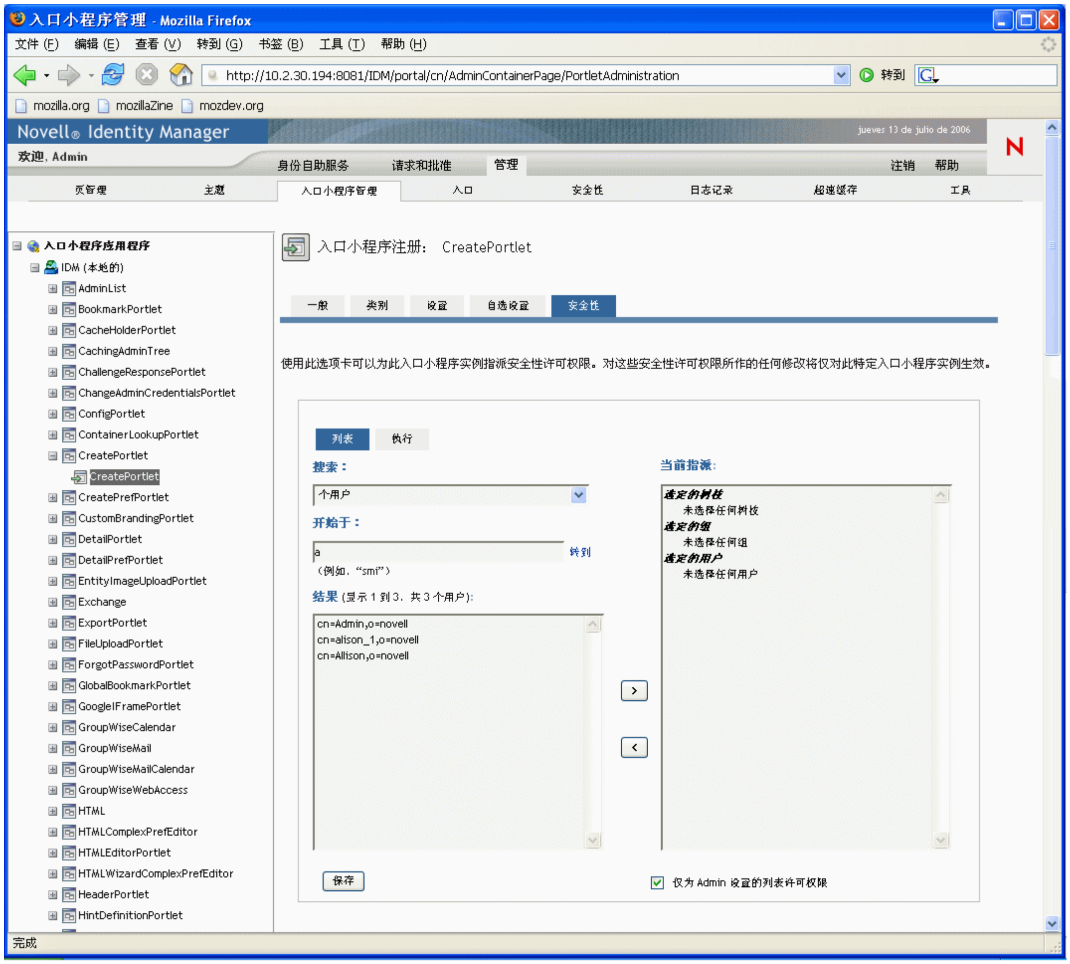
要指派入口小程序注册的安全性许可权限，请执行以下操作：

1 在 《入口小程序应用程序》列表中，选择要修改其安全性许可权限的入口小程序注册。

将在右侧显示 《一般》面板。

2 转至 《安全性》面板。

该面板将显示所选入口小程序注册的当前安全性许可权限：



3 根据要指派的许可权限类型，转至 《列表》或 《执行》选项卡。

4 指定以下搜索设置的值：

设置	操作
搜索主题	从下拉菜单中选择以下项之一： ◆ 用户 ◆ 组 ◆ 树枝

设置	操作

开始于	如果要：
	◆ 查找指定类型 （用户、组或树枝）的**所有**可用对象，请将此处设置为空白。
	◆ 查找这些对象的**子集**，请输入所需的 CN 值的起始字符。 （不区分大小写，不支持通配符。）
	例如，搜索以 S 开头的组将缩小搜索范围，并得到类似以下内容的结果：
	`cn=Sales,ou=groups,o=MyOrg`
	`cn=Service,ou=groups,o=MyOrg`
	`cn=Shipping,ou=groups,o=MyOrg`
	搜索以 Se 开头的组将返回：
	`cn=Service,ou=groups,o=MyOrg`

5 单击 《搜索》。

将在 《结果》列表中显示搜索结果。

6 选择要指派给入口小程序注册的用户、组或树枝，然后单击添加 (>) 按钮。

提示：按住 *Ctrl* 键可选择多项。

7 按照以下说明启用或禁用入口小程序注册的锁定功能：

如果要	操作
锁定入口小程序注册，以便只有用户应用程序管理员才能列出或执行该注册	选中 **List/Execute Permission Set to Admin Only** （仅为 Admin 设置的列出 / 执行许可权限）
允许所有已指派的用户、组和树枝列出或执行入口小程序注册	取消选中 《仅为 Admin 设置的列出 / 执行许可权限》 **注释：**如果取消选中此设置，但没有将用户、组或树枝显式指派给入口小程序注册，则**所有人都将对该注册拥有列出或执行许可权限**。

8 单击 《保存》。

9.4.7 取消注册入口小程序

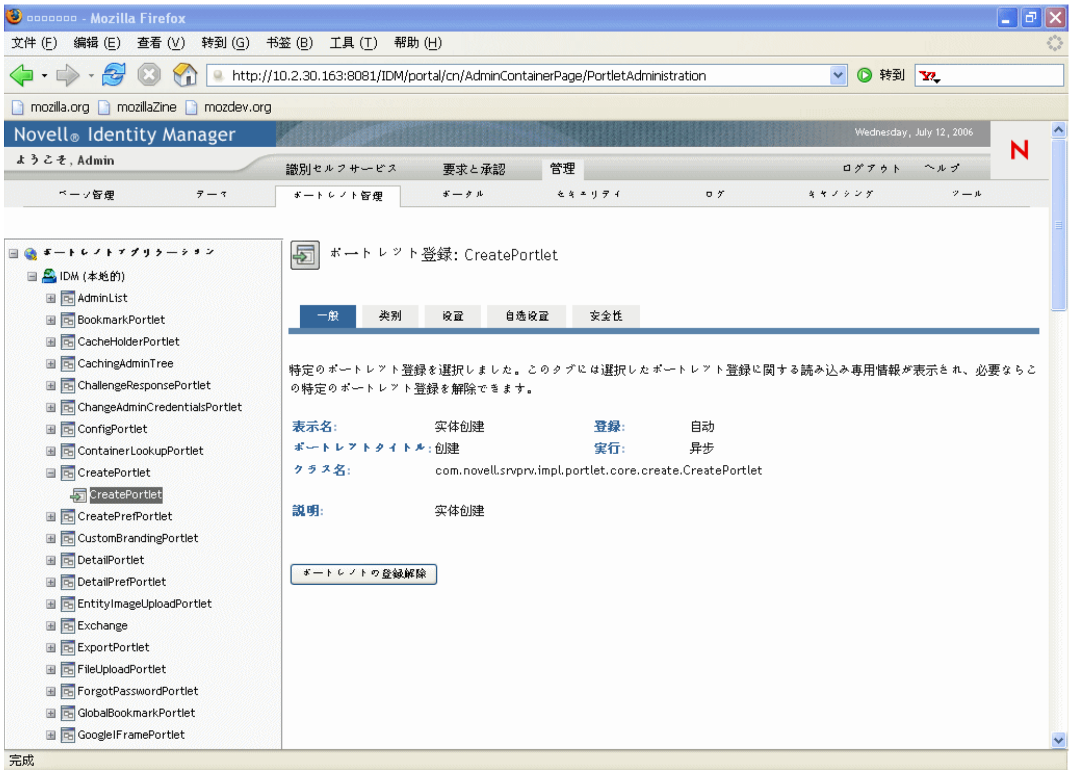
如有必要，可以使用 《入口小程序管理》页取消对入口小程序的注册。

注释：如果将定义为自动注册的入口小程序取消注册，该入口小程序将在重启动应用程序服务器时自动重新注册。

要取消注册入口小程序，请执行以下操作：

1 在 《入口小程序应用程序》列表中，选择要取消其注册的入口小程序注册。

将在右侧显示 《一般》面板，其中将列出有关所选入口小程序注册的信息：



2 单击 《取消注册入口小程序》。

3 当系统提示对取消注册操作进行确认时，请单击 《确定》。

入口配置 10

本章将说明如何使用 Identity Manager 用户界面上 《管理》选项卡的 《入口》页。包括以下主题：

有关访问和使用 《管理》选项卡的更多一般信息，请参见第 6 章 “使用 《管理》选项卡”在第 119 页 。

10.1 关于入口配置

可以使用 《入口》页控制 Identity Manager 用户应用程序的入口特征，并指定此用户应用程序连接到 *Identity Vault* （LDAP 提供程序）的方式。

10.2 一般设置

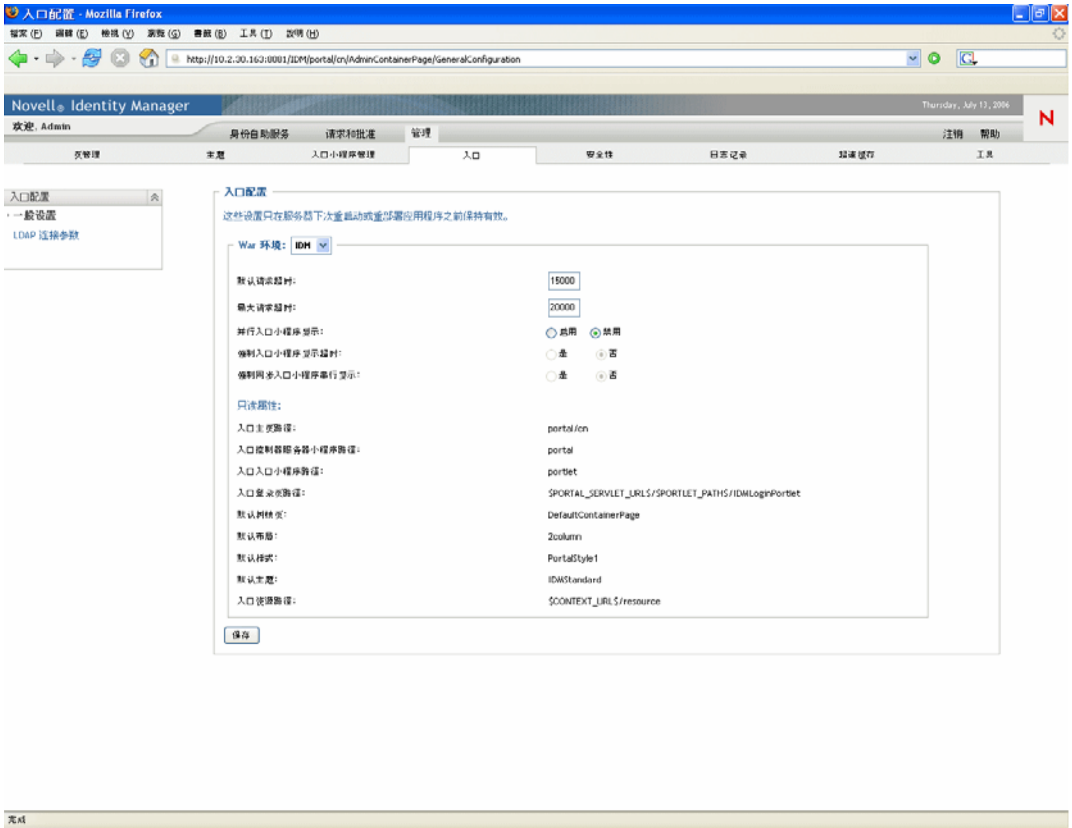
《入口》页提供了 《一般设置》面板，可以通过该面板执行以下操作：

- 临时更改 *Identity Manager* 用户应用程序的某些入口特征 （直到下一次应用程序服务器重启动或用户应用程序重部署）
- 查看 *Identity Manager* 用户应用程序的其它入口特征

要管理一般设置，请执行以下操作：

1 在 《入口》页的左侧导航菜单中，选择 《一般设置》。

将显示 《一般设置》面板：



2 如果 《War 环境》不止一个，请选择希望访问其设置的环境。

面板将随之刷新，并显示所选环境的当前设置。

3 根据需要检查并修改设置。有关详情，请参见：

- “可以更改的设置”在第 184 页
- “只读设置”在第 185 页

4 如果要应用所做的更改，请单击 《保存》。

10.2.1 可以更改的设置

在 《一般设置》面板中，可以修改多项入口设置。所设置的值将一直有效，直到下一次重启动应用程序服务器或重部署用户应用程序。发生重启动或重部署时，这些设置将还原为用户应用程序 WAR 的默认值。

设置	操作
默认请求超时	指定请求超时前将等待的默认时间 （以毫秒为单位）。 如果异步入口小程序均未定义超时，或入口小程序定义的超时均不大于此值，将使用此默认值。如果一个或多个要显示的入口小程序定义的超时大于此默认值，将使用较大的超时值，而不使用默认值。 使用此设置可防止应用程序收到过多指示入口小程序已超时的讯息（当入口小程序定义的值太小时可能会发生这种情况）。 **注释：**如果在此默认超时发生前所有的入口小程序均能显示，则请求将立即返回客户机。
最大请求超时	指定请求完成前经过的最长时间 （以毫秒为单位）。这意味着经过这段时间后，不管是否有任何入口小程序定义了更大的超时值，所有请求都将返回客户机。 使用此设置可以确保入口小程序能够及时响应，即使在一个或多个入口小程序定义了较大超时值的情况下也是如此。
并行入口小程序显示	在入口中启用或禁用异步入口小程序显示。 默认情况下，此高级功能被禁用。如果启用此功能，入口会将异步显示请求指派给独立线程 （这将允许入口小程序并行显示内容）。 禁用此功能时，所有入口小程序都将在主请求线程中同步地显示内容。
强制入口小程序显示超时	决定在线程池中没有足够的可用独立线程时，是否将异步入口小程序委托给主请求线程来显示内容。 如果选择 《否》，则在没有独立线程可用时，异步入口小程序可在主请求线程中执行。 如果选择 《是》，将强制异步入口小程序等待，直到独立线程可用时它们才能显示内容。如果入口小程序在执行显示请求前已超时，将在入口小程序窗口中生成一个入口小程序特有的错误讯息。
强制同步入口小程序串行显示	决定如何执行同步入口小程序。 如果选择 《是》，则所有的同步入口小程序都将在主请求线程中执行。 如果选择 《否》，将允许入口分配独立的线程来处理同步显示请求（从而防止主请求线程中出现瓶颈现象）。

10.2.2 只读设置

显示以下设置只是为了提供信息，不能在 《一般设置》面板中更改它们：

入口主页路径	默认布局
入口控制器服务器小程序路径	默认样式
入口入口小程序路径	默认主题
入口登录页路径	入口资源路径

这些设置的值在用户应用程序 WAR 中设置。（请注意，《默认主题》反映了在《主题》页中选择的当前主题。）

10.3 LDAP 连接参数

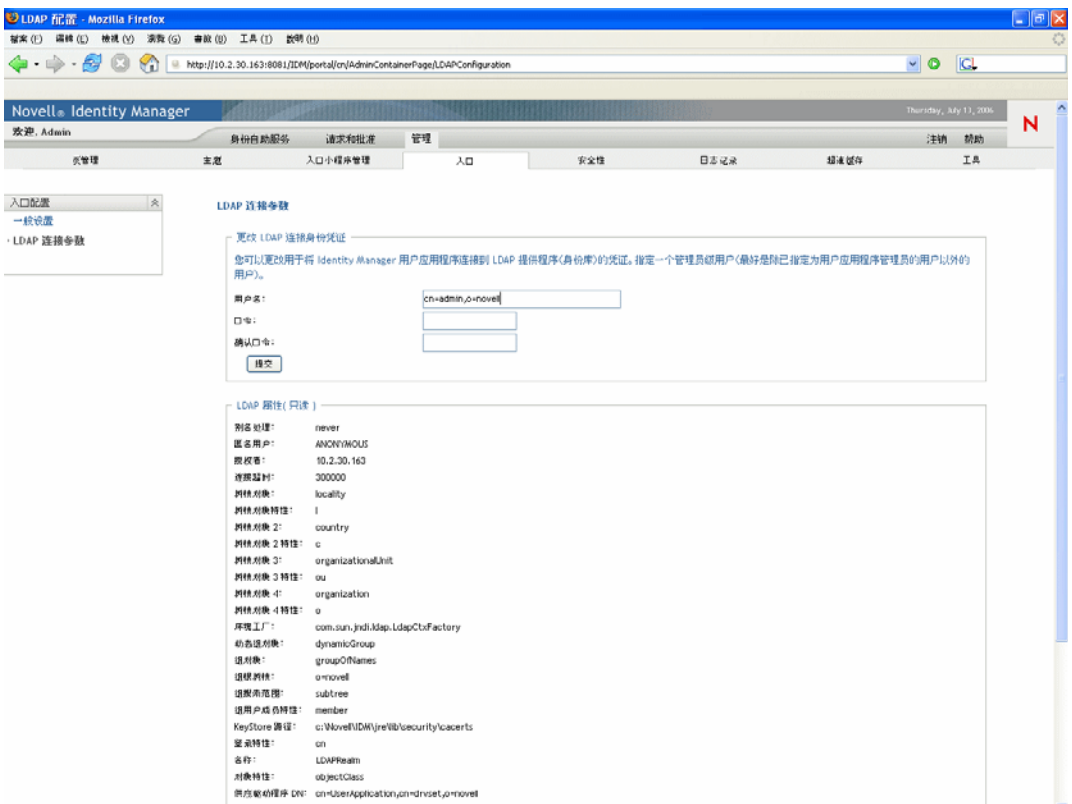
《入口》页提供了一个《LDAP 连接参数》面板，可以使用它进行以下操作：

- 更改 Identity Manager 用户应用程序在连接到 Identity Vault （LDAP 提供程序）时使用的身份凭证
- 查看 Identity Manager 用户应用程序的其它 LDAP 属性

要管理 LDAP 连接参数，请执行以下操作：

1 请在《入口》页的左侧导航菜单中，选择《LDAP 连接参数》。

即显示《LDAP 连接参数》面板：



2 根据需要检查并修改设置。有关详情，请参见：

- "可以更改的设置" 在第 184 页
- "只读设置" 在第 187 页

3 如果要应用所做的更改，请单击《提交》。

10.3.1 可以更改的设置

在 《LDAP 连接参数》面板中，可以修改身份凭证设置，只要 Identity Manager 用户应用程序连接到 Identity Vault （LDAP 提供程序），它就会使用这些身份凭证。在此面板中所做的更改将保存到用户应用程序的数据库中以供运行时使用，并对照 Identity Vault 进行检查。（请注意，该面板不更新在安装期间用户应用程序 WAR 中记录的原始身份凭证值。）

设置	操作
用户名	键入在 Identity Vault 中拥有**管理员**全部权限的用户名。Identity Manager 用户应用程序需要以管理员身份访问 Identity Vault，这样它才能正常运行。 通常指定 Identity Vault 的**根**管理员作为 LDAP 连接用户名。由于根管理员可以全权控制树，因此不需要指派任何特殊的受托者权限。 例如： `cn=admin,o=myorg` 如果指定其它用户，则需要将可继承的受托者权限指派给用户应用程序驱动程序的属性 [All Attributes Rights] 和 [Entry Rights]。 **注释：**为了避免产生混淆，建议**不要**将用户应用程序的用户应用程序管理员指定为 LDAP 连接用户名。最好为这两种不同的情况使用不同的帐户。
口令 和 确认口令	键入在 Identity Vault 中当前为该用户名设置的口令。

10.3.2 只读设置

显示以下设置只为提供信息，不能在 《LDAP 连接参数》面板中更改它们：

ALIAS_HANDLING	GROUP_USER_MEMBER_ATTRIB
ANONYMOUS_USER	KEYSTORE_PATH
AUTHORITY	LOGIN_ATTRIBUTE
CONNECTION_TIMEOUT	NAME
CONTAINER_OBJECT	OBJECT_ATTRIB
CONTAINER_OBJECT_ATTRIB	PROVISION_ROOT
CONTAINER_OBJECT2	REFERRAL
CONTAINER_OBJECT2_ATTRIB	ROOT_NAME
CONTAINER_OBJECT3	USE_DYNAMIC_GROUPS
CONTAINER_OBJECT3_ATTRIB	USE_REGISTERED_DYNAMIC_GROUPS

CONTAINER_OBJECT4	USE_SSL
CONTAINER_OBJECT4_ATTRIB	USER_GROUP_MEMBER_ATTRIB
CONTEXT_FACTORY	USER_OBJECT
DYNAMIC_GROUP_OBJECT	USER_ROOT_CONTAINER
GROUP_OBJECT	USER_SEARCH_SCOPE
GROUP_ROOT_CONTAINER	UUID_ATTRIB
GROUP_SEARCH_SCOPE	UUID_AUX_CLASS

安装用户应用程序时决定这些设置的值。

安全性配置 11

本章介绍如何使用 Identity Manager 用户界面的 《管理》选项卡中的 《安全性》页。包括以下主题：

有关访问和使用 《管理》选项卡的更多一般信息，请参见第 6 章 “使用 《管理》选项卡”在第 119 页 。

11.1 关于安全性配置

可以使用 《安全性》页为 Identity Manager 用户应用程序指定用户应用程序管理员。

用户应用程序管理员有权执行与 Identity Manager 用户应用程序相关的所有管理功能。其中包括通过访问 Identity Manager 用户界面的 《管理》选项卡来执行其支持的所有管理操作。

在安装过程中，指定了作为用户应用程序管理员的用户。安装结束后，该用户可以根据需要使用 《安全性》页指定其他用户应用程序管理员。

通常情况下，要作为用户应用程序管理员的用户应该位于用户根树枝下，该根树枝在用户应用程序的 LDAP 配置中指定；这使得该用户只需通过用户名即可登录 （而不是每次都需要使用完整的判别名）。通常，该用户还拥有在树中维护和创建对象的权限，但并不需要这样做。

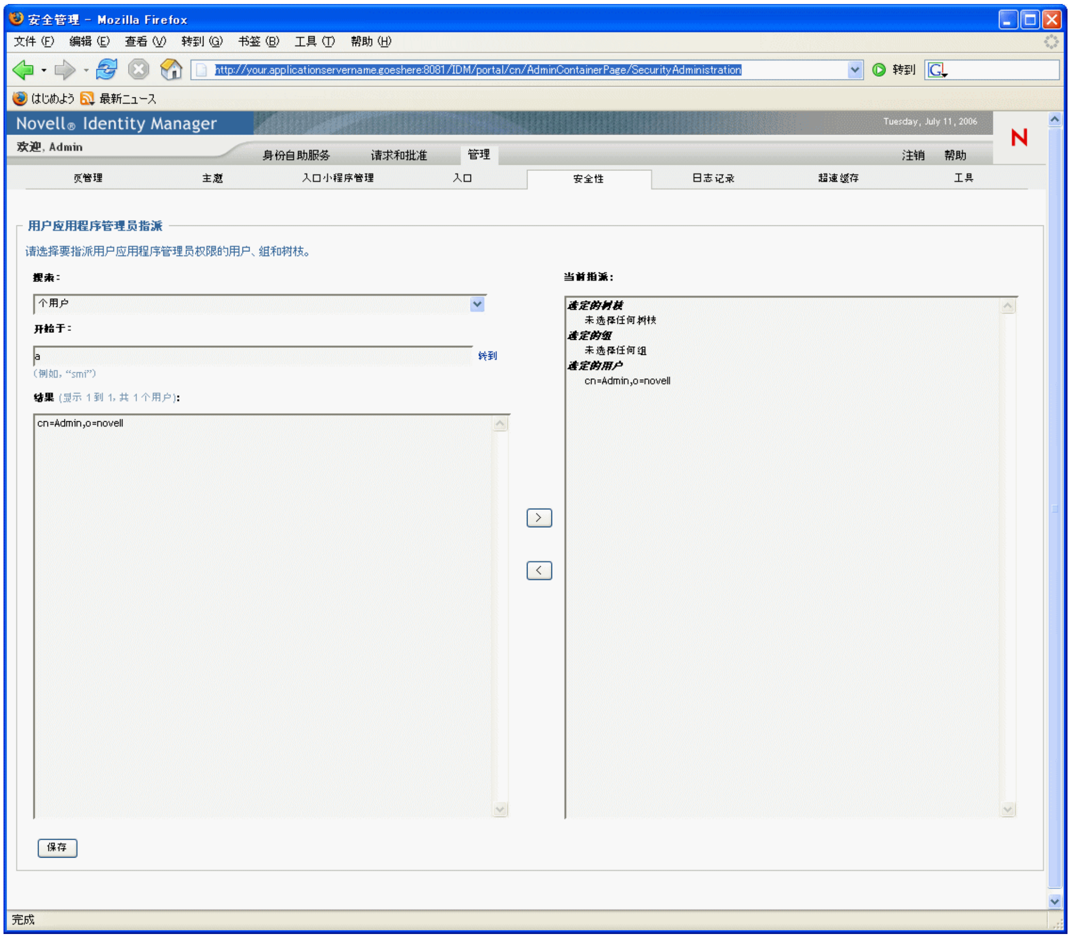
注释 : 如有必要，用户应用程序管理员可以将许可权限指派给一个或多个终端用户，使其可以查看并访问 《管理》选项卡上的特定页。使用 《管理》选项卡中的 《页管理》页可指派这些许可权限。（有关详情，请参见第 7 章 “页管理”在第 125 页 。）

11.2 指派用户应用程序管理员

指派用户应用程序管理员时，可以指定用户、组或树枝。

要指派用户应用程序管理员，请执行以下操作：

1 转至《安全性》页：



2 指定以下搜索设置的值：

设置	操作
搜索主题	从下拉菜单中选择以下项之一： ◆ 用户 ◆ 组 ◆ 树枝

设置	操作

开始于	如果要：
	◆ 查找指定类型 （用户、组或树枝）的**所有**可用对象，请将此处设置为空白。
	◆ 查找这些对象的**子集**，请输入所需的 CN 值的起始字符。 （不区分大小写，不支持通配符。）
	例如，搜索以 S 开头的组将缩小搜索范围，并得到类似以下内容的结果：
	`cn=Sales,ou=groups,o=MyOrg`
	`cn=Service,ou=groups,o=MyOrg`
	`cn=Shipping,ou=groups,o=MyOrg`
	搜索以 Se 开头的组将返回：
	`cn=Service,ou=groups,o=MyOrg`

3 单击 《搜索》。

将在 《结果》列表中显示搜索结果。

4 选择要指派为用户应用程序管理员的用户、组或树枝，然后单击添加 (>) 按钮。

提示 **:** 按住 *Ctrl* 键可选择多项。

5 单击 《保存》。

要取消指派用户应用程序管理员，请执行以下操作：

1 在 《当前指派》列表中，选择想要取消指派为用户应用程序管理员的用户、组或树枝，然后单击去除 (<) 按钮。

提示 **:** 按住 *Ctrl* 键可选择多项。

2 单击 《保存》。

日志记录配置 12

本章介绍如何使用 Identity Manager 用户界面的 《管理》选项卡中的 《日志记录》页。包括以下主题：

有关访问和使用 《管理》选项卡的更多一般信息，请参见第 6 章 "使用 《管理》选项卡"在第 119 页 。

12.1 关于日志记录配置

可以使用 《日志记录》页来控制希望 Identity Manager 用户应用程序生成的日志记录讯息的级别，并指定是否要将这些讯息发送至 *Novell Audit*。

Identity Manager 用户应用程序使用由 Apache Software Foundation 分发的开放源代码日志记录包 *log4j* 实施日志记录。默认情况下，事件讯息会同时记录到下面两个位置：

- 部署 Identity Manager 用户应用程序的应用程序服务器的系统控制台。
- 该应用程序服务器上的日志文件，例如：

```
jboss/server/IDM/log/server.log
```

这是一个滚动日志文件，当它达到一定大小时，将滚动至另一个文件 （依此类推）。

如果已将环境配置为包含 Novell Audit，则还可以选择将事件讯息记录到 Novell Audit 中。

有关配置日志记录环境和 Novell Audit 的详情，请参见第 5 章 "设置日志记录"在第 109 页 。

12.2 关于日志

《日志记录》页列出了各种不同的日志，每个日志都从 Identity Manager 用户应用程序的不同部分输出事件讯息。每个日志都有其独立的输出级别。

日志名称基于 log4j 约定。在生成的事件讯息中可以看到这些日志名称，这些名称指示了讯息输出的环境。

日志名称	说明
com.novell	其它 Identity Manager 用户应用程序日志的父级
com.novell.afw.portal.aggregation	与入口页处理有关的讯息

日志名称	说明
com.novell.afw.portal.persist	与入口数据的持续性有关的讯息 （包含入口页和入口小程序注册）
com.novell.afw.portal.portlet	来自入口内核入口小程序和附属入口小程序的讯息
com.novell.afw.portal.util	来自入口导入 / 导出和导航入口小程序的讯息
com.novell.afw.portlet.consumer	与入口小程序显示有关的讯息
com.novell.afw.portlet.core	与内核入口小程序 API 有关的讯息
com.novell.afw.portlet.persist	与入口小程序数据 （包括入口小程序自选设置和设置值）的持续性有关的讯息
com.novell.afw.portlet.producer	与入口内入口小程序的注册和配置有关的讯息
com.novell.afw.portlet.util	与入口小程序使用的实用程序代码有关的讯息
com.novell.afw.theme	来自主题子系统的讯息
com.novell.afw.util	与入口实用程序类有关的讯息
com.novell.soa.af.impl	来自批准流程 （供应工作流程）子系统的讯息
com.novell.srvprv.apwa	来自 《请求和批准》万维网应用程序的讯息 （操作和标签）
com.novell.srvprv.impl.portlet.core	来自内核身份入口小程序和口令入口小程序的讯息
com.novell.srvprv.impl.portlet.util	来自与身份相关的实用程序入口小程序的讯息
com.novell.srvprv.impl.servlet	来自 UI 控件框架的 ajax 服务器小程序和 ajax 服务的讯息
com.novell.srvprv.impl.uictrl	来自 UI 控件注册表 API 和批准表单显示的讯息
com.novell.srvprv.impl.vdata	来自目录提取层的讯息
com.novell.srvprv.spi	来自 UI 控件注册表 API 的讯息
com.sssw.fw.cachemgr	与框架超速缓存子系统有关的讯息
com.sssw.fw.core	与框架内核子系统有关的讯息
com.sssw.fw.directory	与框架目录子系统有关的讯息
com.sssw.fw.event	与框架事件子系统有关的讯息
com.sssw.fw.factory	与框架工厂子系统有关的讯息
com.sssw.fw.persist	与框架持续性子系统有关的讯息
com.sssw.fw.resource	与框架资源子系统有关的讯息
com.sssw.fw.security	与框架安全性子系统有关的讯息
com.sssw.fw.server	与框架服务器子系统有关的讯息
com.sssw.fw.servlet	与框架服务器小程序子系统有关的讯息
com.sssw.fw.session	与框架会话子系统有关的讯息
com.sssw.fw.usermgr	与框架用户子系统有关的讯息
com.sssw.fw.util	与框架实用程序子系统有关的讯息

日志名称	说明
com.sssw.portal.manager	与入口管理器有关的讯息
com.sssw.portal.persist	与入口持续性有关的讯息

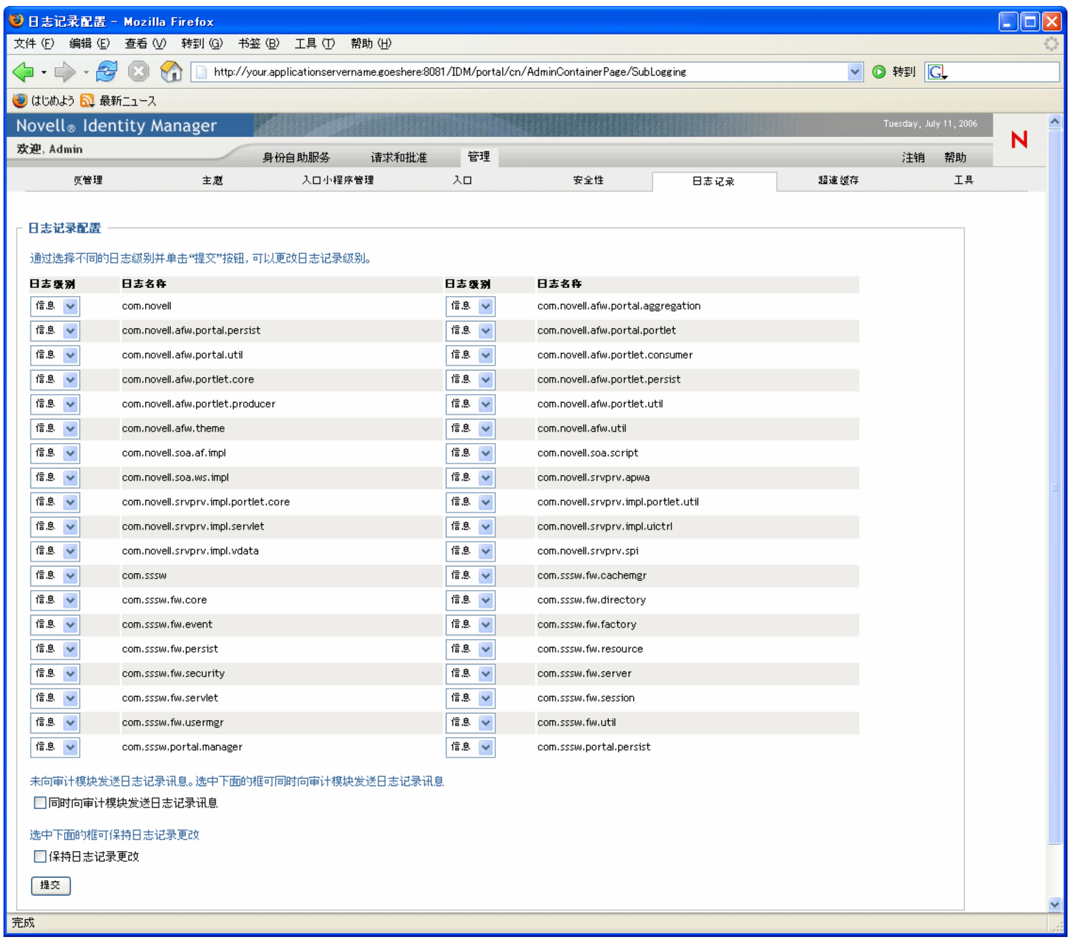
请注意，用户应用程序的日志是分级的。例如， com.novell 为在它下面的其它日志的父级。任何附加日志都将继承它的属性。

12.3 更改日志级别

可以通过更改为特定日志设置的级别来控制写入该日志的信息量。默认情况下，所有的日志都设置为 《信息》，这是一个中间级别。

要更改日志级别，请执行以下操作：

1 转至 《日志记录》页：



2 在页面顶部，查找日志以更改其级别。

3 使用下拉列表选择以下级别之一：

级别	说明
致命错误	**最不详细：**
	将致命错误写入日志
错误	将错误 （和以上级别的所有内容）写入日志
警告	将警告 （和以上级别的所有内容）写入日志
信息	将信息性讯息 （和以上级别的所有内容）写入日志
调试	将调试信息 （和以上级别的所有内容）写入日志
跟踪	**最为详细：**
	将跟踪信息 （和以上级别的所有内容）写入日志

4 根据需要，对其它日志重复执行 步骤 2 和步骤 3。

5 单击 《提交》。

12.4 将日志讯息发送至 Novell Audit

可以使用 《日志记录》页控制 Identity Manager 用户应用程序是否将事件讯息输出发送至 Novell Audit。默认情况下， Novell Audit 日志记录处于关闭状态，除非在安装用户应用程序时将它打开。

要使 Novell Audit 日志记录在打开 / 关闭之间切换，请执行以下操作：

1 转至 《日志记录》页。

2 根据需要，选中或取消选中下面的设置：

```
Also send logging messages to Audit
```

3 单击 《提交》。

12.5 保持日志设置

默认情况下，在 《日志记录》页上进行的更改在下一次重启动应用程序服务器或重新部署用户应用程序之前一直有效。之后，日志设置会恢复为它们的默认值。

但 《日志记录》页确实提供了保持对其设置的更改这样的选项。如果打开此功能，日志设置的值会储存在部署 Identity Manager 用户应用程序的应用程序服务器上的日志记录配置文件中。例如：

```
jboss/server/IDM/conf/extendlogging.xml
```

要使保持设置在打开 / 关闭之间切换，请执行以下操作：

1 转至 《日志记录》页。

2 根据需要，选中或取消选中下面的设置：

```
Persist the logging changes
```

3 单击 《提交》。

超速缓存配置 13

本章介绍如何使用 Identity Manager 用户界面的 《管理》选项卡中的 《超速缓存》页。包括以下主题：

有关访问和使用 《管理》选项卡的更多一般信息，请参见第 6 章 “使用 《管理》选项卡”在第 119 页 。

13.1 关于超速缓存配置

可以使用 《超速缓存》页来管理 Identity Manager 用户应用程序维护的各种超速缓存。用户应用程序使用这些超速缓存来储存应用程序服务器上可重用的临时数据，以便优化性能。

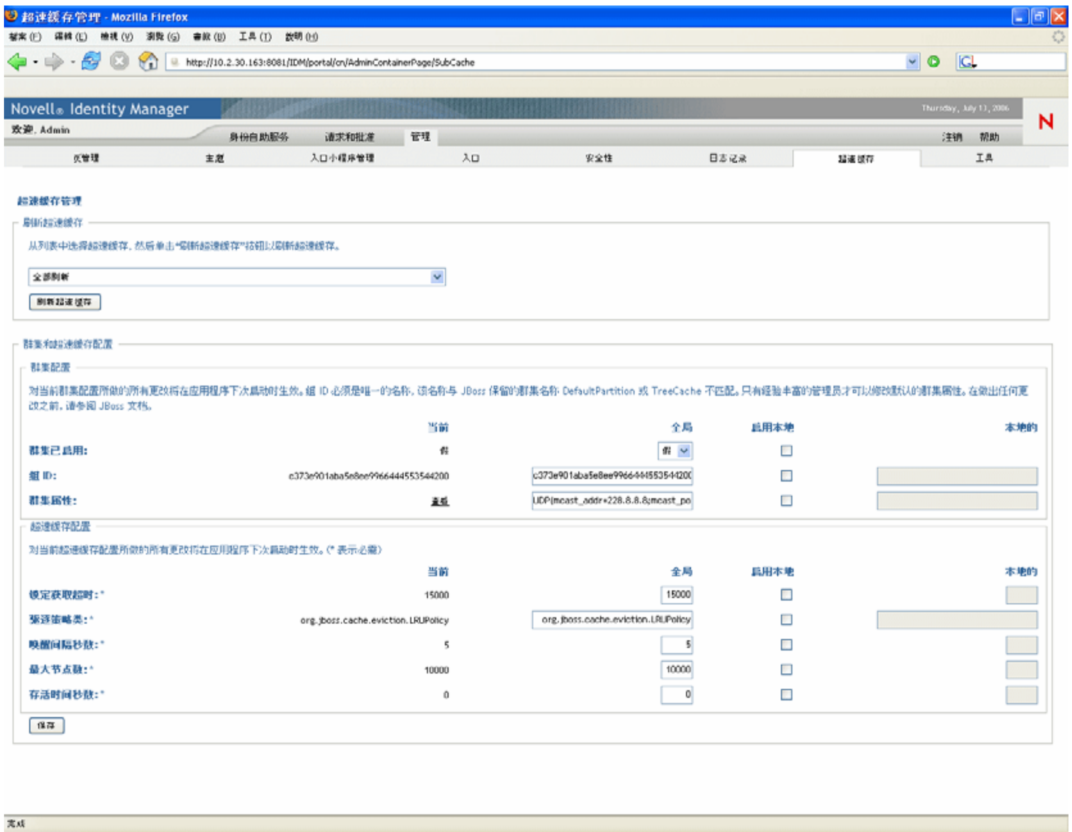
必要时，可以通过清理超速缓存中的内容以及更改其配置设置来控制这些超速缓存。

13.2 清理超速缓存

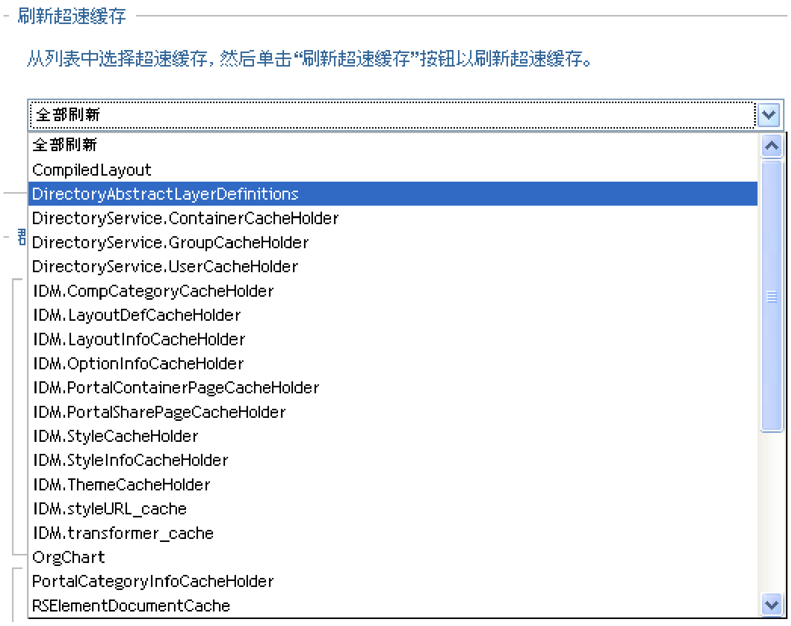
超速缓存是根据在 Identity Manager 用户应用程序中使用它们的子系统而命名的。由于用户应用程序会根据它们的数据使用频率或源数据更改时间自动清理它们，因此通常情况下，无需亲自清理它们。但如有特殊要求，可以手动清理选定的超速缓存或所有超速缓存。

要清理超速缓存，请执行以下操作：

1 转至 《超速缓存》页：



2 在该页的 *Flush Cache* （清理超速缓存）部分，使用下拉列表选择要清理的特定超速缓存 （或选择 *Flush all* （清理全部））：



请注意，可用超速缓存的列表是动态的，该列表会随时根据所超速缓存的数据而变化。

3 单击 《清理超速缓存》按钮。

13.2.1 清理目录提取层超速缓存

用户应用程序的目录提取层也有超速缓存。*DirectoryAbstractLayerDefinitions* 超速缓存储存应用程序服务器中的提取层定义，以优化所有数据模型操作的性能。

一般情况下，用户应用程序将自动在 DirectoryAbstractLayerDefinitions 超速缓存与储存在 Identity Vault 中的提取层定义之间保持同步。但如果需要，可以手动清理 DirectoryAbstractLayerDefinitions 超速缓存 （如上所述）以强制从 Identity Vault 中装载最新定义。

有关用户应用程序的目录提取层的更多信息，请参见第 4 章 “配置目录提取层” 在第 69 页 。

13.2.2 清理群集中的超速缓存

群集的和非群集的应用程序服务器环境都支持超速缓存清理。如果应用程序服务器是群集的一部分，并且手动清理超速缓存，将在群集中的每个服务器上自动清理该超速缓存。

13.3 配置超速缓存设置

可以使用 《超速缓存》页显示和更改群集的或非群集的应用程序服务器环境的超速缓存配置设置。所做的更改会立即保存，但在下一次重启动用户应用程序时才生效。

提示：要重启动用户应用程序，可以执行以下操作之一：重引导应用程序服务器、重新部署应用程序（如果以某种方式更改了 WAR）、或强制应用程序重启动（按照应用程序服务器文档中的描述）。

要配置超速缓存设置，需要了解：

- “如何实现超速缓存”在第 202 页
- “如何储存超速缓存设置”在第 202 页
- “如何显示超速缓存设置”在第 203 页
- “基本超速缓存设置”在第 204 页
- “群集的超速缓存设置”在第 205 页

13.3.1 如何实现超速缓存

在 Identity Manager 用户应用程序中，超速缓存是通过 *JBoss* 超速缓存实现的。JBoss 超速缓存是 JBoss 应用程序服务器附带的开放源代码超速缓存体系结构，但它也可以在其它应用程序服务器上运行。

要了解有关 JBoss 超速缓存的更多信息，请访问 www.jboss.org/products/jbosscache (http://www.jboss.org/products/jbosscache)。

13.3.2 如何储存超速缓存设置

有两种级别的设置可用于控制超速缓存配置。可以结合使用它们以自定义 Identity Manager 用户应用程序的超速缓存行为。

级别	说明

全局设置	全局设置**储存在中心位置** (Identity Vault)，以便多个应用程序服务器能够使用相同的设置值。例如，使用应用程序服务器群集的人通常会使用群集配置值的全局设置。
	
	若要在 Identity Vault 中**查找全局设置**，请在 Identity Manager 用户应用程序驱动程序中查找下面的对象：
	
	`configuration.AppDefs.AppConfig`
	
	例如：
	
	`configuration.AppDefs.AppConfig.MyUserApplicationDriver.MyDriverSet.MyOrg`
	
	配置对象的 **XmlData 特性**包含全局设置数据。

级别	说明

本地设置	本地设置**单独储存在每个应用程序服务器上**，以便单个服务器可以**覆盖**一个或多个全局设置的值。例如，可能希望指定一个本地设置以从全局设置中指定的群集中去除某个应用程序服务器，或将某个服务器重指派给其它群集。
	
	若要在应用程序服务器中**查找本地设置**，请在 JBoss 服务器配置的 conf 目录下查找下面的文件：
	
	`sys-configuration-xmldata.xml`
	
	例如：
	
	`jboss/server/IDM/conf/sys-configuration-xmldata.xml`
	
	如果服务器有本地设置，则相应数据会包含在此文件中。（如果未指定本地设置，则此文件不存在。）

应将全局设置视为使用用户应用程序驱动程序特定实例的每个应用程序服务器的默认值。更改全局设置时，这些服务器中的每一个都会受到影响 （在下一次重启动用户应用程序时），但那些指定了本地覆盖设置的个别服务器除外。

13.3.3 如何显示超速缓存设置

《超速缓存》页显示了当前超速缓存设置 （从上一次重启动用户应用程序时开始）。它还显示了这些设置的相应全局和本地值，还可以更改这些值 （以便下一次重启动用户应用程序时使用）。



请注意，全局设置始终是有值的。本地设置为可选项。

13.3.4 基本超速缓存设置

这些超速缓存设置同时应用于群集和非群集的应用程序服务器。

要配置基本超速缓存设置，请执行以下操作：

1 转至 《超速缓存》页。

2 在该页的 《超速缓存配置》部分，根据需要为下列设置指定全局或本地值：

设置	操作
锁定获取超时	指定超速缓存为获取对对象的锁定而需等待的**时间间隔 （以毫秒为单位）**。如果用户应用程序在应用程序日志中得到大量的锁定超时异常，则可能需要增大此设置。默认值为 15000 ms。
驱逐策略类	指定想要使用的超速缓存驱逐策略的**类名**。默认值为 JBoss 超速缓存提供的 LRU 驱逐策略： `org.jboss.cache.eviction.LRUPolicy` 可以根据需要将此默认驱逐策略更改为 JBoss 超速缓存支持的其它驱逐策略。 若要了解受支持的驱逐策略，请访问 www.jboss.org/products/jbosscache (http://www.jboss.org/products/jbosscache)。
唤醒间隔秒数	指定在唤醒超速缓存驱逐策略以执行以下操作前超速缓存驱逐策略等待的**时间间隔 （以秒为单位）**： ◆ 处理驱逐节点事件 ◆ 清理大小限制和老化节点
最大节点数	指定超速缓存中允许的**最大节点数**。如果没有限制，请指定： `0`
到有效秒数的时间	指定节点清除前的**空闲时间 （以秒为单位）**。如果没有限制，请指定： `0`

这些设置是必需的，这意味着每个设置都必须有一个全局值，同时也可以有一个本地值。

如果想要使用本地值覆盖设置的全局值，请选中该设置的 《启用本地》复选框。然后指定本地值。 （请确保所有本地值都有效。否则，将无法保存所做的更改。）

注释 : 对于那些未选中 《启用本地》的设置，保存时将删除现有的本地值。

3 单击 《保存》。

4 要使保存的设置生效，请在相应的应用程序服务器上重启动用户应用程序。

13.3.5 群集的超速缓存设置

本节讨论在应用程序服务器的群集中运行 Identity Manager 用户应用程序时如何配置超速缓存。需要了解：

- "如何实现群集"在第 205 页
- "如何将超速缓存用于群集"在第 205 页
- "准备使用群集"在第 205 页
- "配置群集的超速缓存设置"在第 206 页

如何实现群集

在 Identity Manager 用户应用程序中，通过 *JGroups* 实现对超速缓存的群集支持。JGroups 是 JBoss 应用程序服务器附带的开放源代码群集体系结构，但它也可以在其它应用程序服务器上运行。

用户应用程序的群集由运行 JGroups 并使用通用组 *ID* 的网络节点组成。默认情况下，为用户应用程序的群集提供的组 ID 为 UUID，如下所示：

```
c373e901aba5e8ee9966444553544200
```

UUID 有助于确保唯一性，以使用户应用程序群集的组 ID 不会与环境中其它群集的组 ID 发生冲突。例如， JBoss 应用程序服务器本身使用两个 JGroups 群集，并为它们保留组 *ID DefaultPartition* 和 *TreeCache*。

要了解有关 JGroups 的更多信息，请访问 www.jboss.org/products/jgroups (http://www.jboss.org/products/jgroups)。

如何将超速缓存用于群集

启动用户应用程序时，应用程序的超速缓存配置设置决定是否参与群集以及是否将超速缓存更改复制到该群集中的其它节点。如果启用群集，则在发生更改时，用户应用程序将通过向每个节点发送超速缓存项失效讯息来完成这种复制。

准备使用群集

要在群集中使用超速缓存，需要执行两个主要步骤：

1 设置 *JGroups* 群集

这包括安装 JBoss 应用程序服务器以使用所有的配置，然后将 Identity Manager 用户应用程序 (IDM.war) 分布到群集中的每个服务器，通常的做法是将其放在 *farm* 目录中。

2 在用户应用程序的超速缓存配置设置中启用该群集的使用

请参见"配置群集的超速缓存设置"在第 206 页 （下文）。

配置群集的超速缓存设置

准备好可以使用的群集后，就可以指定设置以在该群集中支持超速缓存。

要配置群集超速缓存设置，请执行以下操作：

1 转至 《超速缓存》页。

2 在该页的 《群集配置》部分，根据需要为下列设置指定全局或本地值：

设置	操作
启用群集	选择 **True** 以将超速缓存更改复制到组 ID 指定的群集中的其它节点。如果不希望参与群集，请选择 **False**。
组 ID	指定想要参与的 JGroups 群集的组 ID。**除非想要使用不同的群集**，否则**没有必要更改**为用户应用程序的群集提供的默认组 ID。 请记住，下列组 ID 保留用于 JBoss 应用程序服务器：DefaultPartition 和 TreeCache。 提示 **:** 若要在日志记录讯息中查看组 ID，请确保将超速缓存日志的级别 (com.sssw.fw.cachemgr) 设置为 《信息》或更高。
群集属性	为群集指定 JGroups **协议堆栈**，该群集由组 ID 指定。请注意，此设置是供可能需要调整群集属性的**有经验的管理员**使用的。否则，不应更改默认的协议堆栈。 要查看当前的群集属性，请单击 《查看》。 有关 JGroups 协议堆栈的详情，请访问 www.joss.org/wiki/Wiki.jsp?page=JGroups (http://www.jboss.org/wiki/Wiki.jsp?page=JGroups)。

如果想要使用本地值覆盖设置的全局值，请选中该设置的 《启用本地》复选框。然后指定本地值。

注释 **:** 对于那些未选中 《启用本地》的设置，保存时将删除现有的本地值。

确保群集中的所有节点指定相同的组 ID 和群集属性。 （若要查看特定节点的这些设置，必须访问在该节点上运行的 Identity Manager 用户界面 - 通过浏览至该服务器上用户界面的 URL - 然后显示 《超速缓存》页。）

3 单击 《保存》。

4 要使保存的设置生效，请在相应的应用程序服务器上重启动用户应用程序。

用于导出和导入入口数据的工具 14

本章介绍如何使用 Identity Manager 用户界面的 《管理》选项卡上的 《工具》页。包括以下主题：

- "关于导出和导入入口数据"在第 207 页
- "导出入口数据"在第 208 页
- "导入入口数据"在第 210 页

有关访问和使用 《管理》选项卡的更多一般信息，请参见第 6 章 "使用 《管理》选项卡"在第 119 页。

14.1 关于导出和导入入口数据

可以使用 《工具》页导入或导出在 Identity Manager 用户应用程序中使用的入口内容 （页和入口小程序）。此内容也称为入口配置状态，它包含：

- 树枝和共享页 （包含每个页所指派的入口小程序和每个入口小程序的自选设置和设置）
- 入口小程序注册

可以使用导入和导出工具根据需要将入口配置状态从一个入口 （用户应用程序）移动至另一个入口。以下是这些工具的工作原理：

工具	工作原理
入口数据导出	生成一组选定树枝和共享页以及入口小程序的 XML 描述。这些 XML 文件储存在可用作入口数据导入工具输入的**入口数据导出 ZIP** 文件中。
入口数据导入	接受入口数据导出 ZIP 文件作为输入。使用入口数据导出 ZIP 文件生成树枝和共享页以及入口 （用户应用程序）中的入口小程序。

14.1.1 用途

可以使用入口数据导出 / 导入工具进行以下操作：

- 将入口配置状态从测试 （源）环境移动至生产 （目标）环境
- 逐渐更新入口的配置状态
- 克隆入口
- 重写目标入口的配置状态 （可选）

14.1.2 要求

要使用入口数据导出 / 导入工具，请确保 Identity Manager 用户应用程序 （入口）在源和目标应用程序服务器上已部署并正在运行。

源和目标服务器不需要访问相同的 *Identity Vault* ；它们可以根据需要访问不同的 Identity Vault。这些 Identity Vault 中的用户、组和树枝不需要是相同的。

14.1.3 限制

不能使用入口数据导出 / 导入工具执行以下操作：

- 当前服务器为用户请求提供服务时，导出或导入入口配置状态
- 导出或导入入口类和资源
- 导出或导入入口小程序类和资源
- 导出或导入用于入口的身份和供应数据
- 导出或导入不是用于页和入口小程序的管理设置
- 从入口的较低版本向较高版本迁移配置状态 （入口必须是相同版本）

14.1.4 步骤

要导出和导入入口数据，请执行以下操作：

1. 如果要执行递增更新，则备份目标入口。
2. 在源入口，使用入口数据导出工具导出入口数据。
   请参见 "导出入口数据" 在第 208 页 。
3. 在目标入口，使用入口数据导入工具导入入口数据。
   请参见 "导入入口数据" 在第 210 页 。
4. 测试目标入口以确保导入了期望导入的数据。

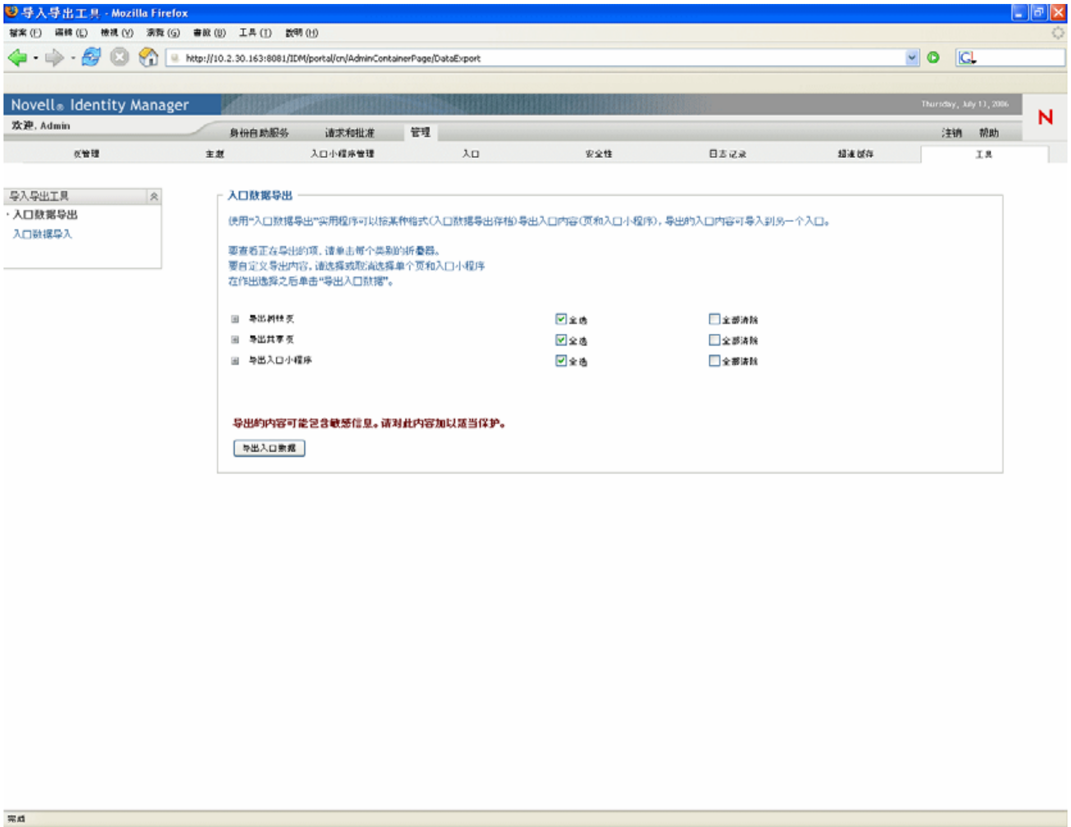
14.2 导出入口数据

本节说明如何将入口配置状态导出到入口数据导出 ZIP 文件。

要导出入口数据，请执行以下操作：

1. 在 《工具》页左侧的导航菜单中选择 《入口数据导出》。

将显示 《入口数据导出》面板：



2 按照屏幕指导选择要导出的入口页和入口小程序。

注释 : 某些未选择导出的入口小程序仍可能会导出。如果导出页中包含的入口小程序为未选择导出的入口小程序，则仍然会导出该入口小程序 （以确保导出页不会发生运行时错误）。

---

3 完成选择后，单击 《导出入口数据》按钮。

将生成新的入口数据导出 *ZIP* 文件，其默认名称中包括当前日期和时间。例如：

```
PortalData.21-Oct-05.09.12.16.zip
```

随后系统将提示在本地保存此 ZIP 文件 （或在适当的存档实用程序中打开它）。例如：



4 将入口数据导出 ZIP 文件保存到适当位置。

14.3 导入入口数据

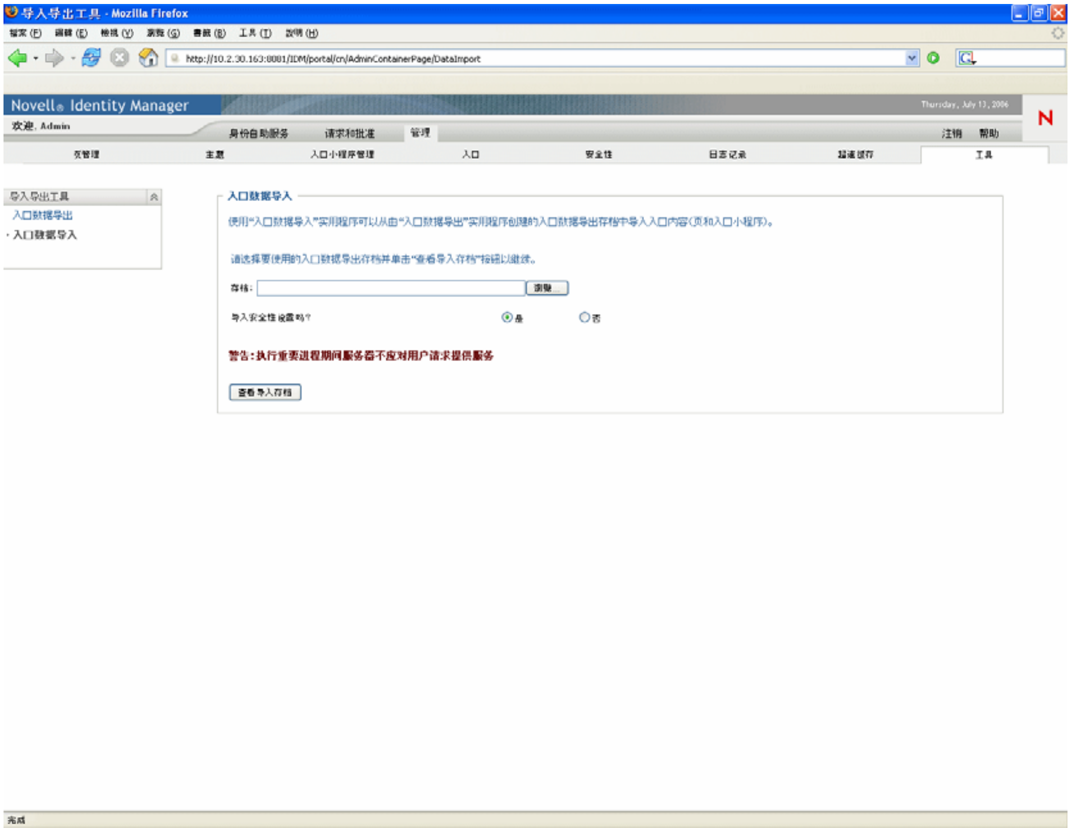
本节说明如何将入口数据 ZIP 文件导入到入口。

注释：请记住，在导入期间，目标应用程序服务器必须保持运行，但当前不为用户请求提供服务。

要导入入口数据，请执行以下操作：

1 在 《工具》页左侧的导航菜单中选择 《入口数据导入》。

将显示《入口数据导入》面板：

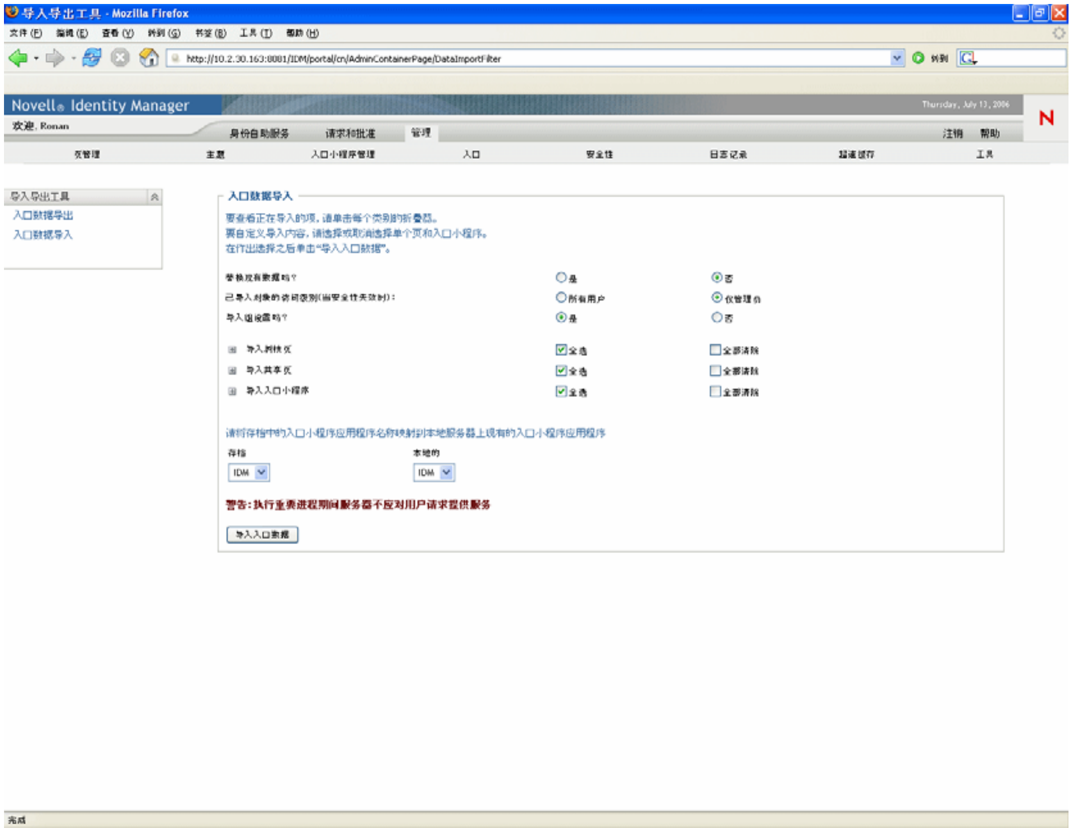


2 指定以下一般导入设置：

设置	操作
存档	单击《浏览》按钮，选择要导入的**入口数据导出 ZIP 文件**。例如： `PortalData.21-Oct-05.09.12.16.zip`
导入安全性设置吗？	请选择以下项之一： ◆ **是** - 如果要导入入口数据导出 ZIP 文件为用户、组和树枝访问页和入口小程序指定的许可权限。请确保相关的用户、组和树枝存在于目标入口的 Identity Vault 中；无法为不存在的实体导入许可权限。 ◆ 否 - 如果希望忽略入口数据导出 ZIP 文件指定的许可权限。

3 单击《查看导入存档》按钮。

面板中显示有关选定的入口数据导出 ZIP 文件以及导入方式的更多具体内容：



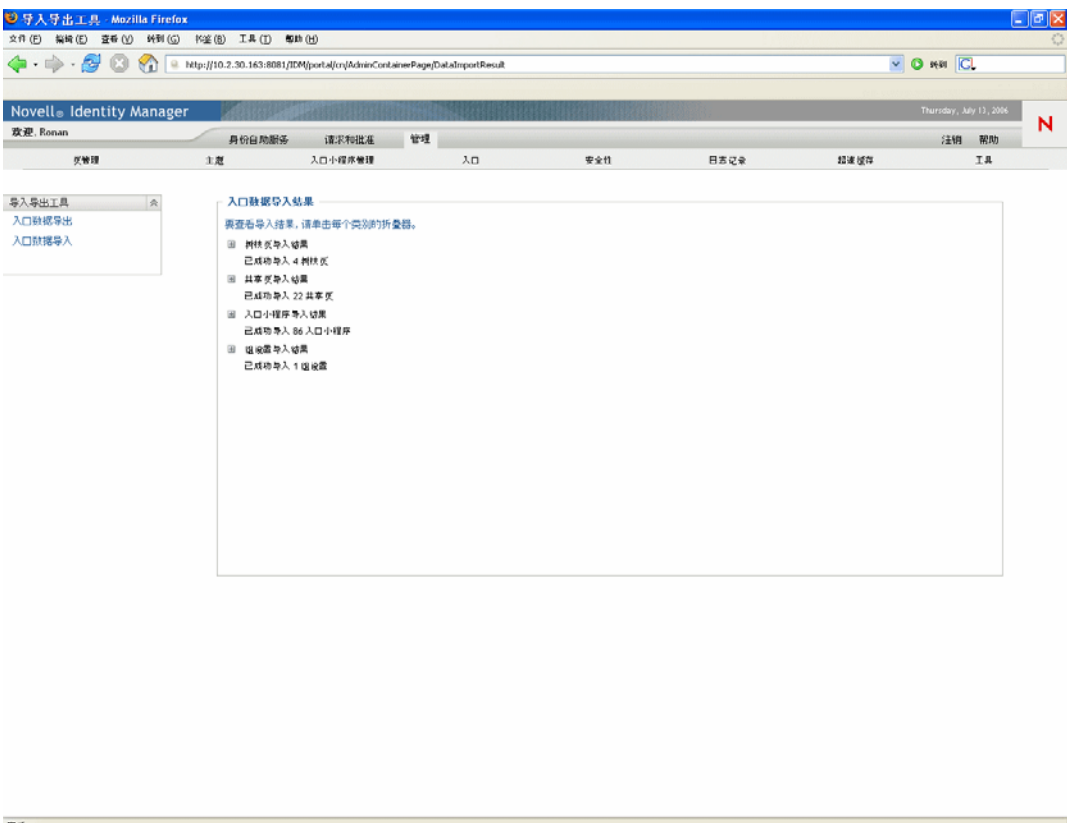
4 指定以下详细导入设置：

设置	操作
替换现有数据吗？	请选择以下项之一： ◆ **是** - 如果希望用入口数据导出 ZIP 文件的内容覆盖已存在于目标入口中的相应的页和入口小程序。例如，如果入口数据导出 ZIP 文件中包含名为 MyPage 的共享页，且目标入口中也包含名为 MyPage 的共享页，则将覆盖目标入口中的现有页。 ◆ **否** - 如果希望跳过对所有现有的页和入口小程序进行的导入。
已导入对象的访问级别	请选择以下项之一： ◆ **所有用户** - 不限制对已导入页和入口小程序的访问。 ◆ **仅管理员** - 对已导入的页和入口小程序进行有限制的访问。 **如果选择导入安全性设置**，则此访问级别仅应用于那些未能导入安全性设置的已导入页和入口小程序（通常是因为目标入口的 Identity Vault 中不存在指定的用户、组或树枝）。 **如果选择不导入安全性设置**，则此访问级别应用于所有已导入的页和入口小程序。

设置	操作
导入组设置吗？	（如果选择导入安全性设置）请选择以下项之一： ◆ **是** - 如果要导入入口数据导出 ZIP 文件为组指定的默认树枝页和默认共享页指派。请确保目标入口的 Identity Vault 中存在相关的组；无法导入不存在的组的指派。 ◆ **否** - 如果要忽略入口数据导出 ZIP 文件为组指定的默认页指派。
导入树枝页 导入共享页 导入入口小程序	按屏幕指导**选择页和入口小程序**，将其从入口数据导出 ZIP 文件导入目标入口。 **注释：**某些未选择导入的入口小程序仍可能会导入。如果导入页中包含的入口小程序为未选择导入的入口小程序，则仍然会导入该入口小程序（以确保已导入页不会发生运行时错误）。
请映射入口应用程序名称 ... 存档 / 本地	使用 《存档》和 《本地》下拉菜单，将存档 （入口数据导出 ZIP 文件）中的入口小程序应用程序名称映射到本地 （目标）应用程序服务器中现有的入口小程序应用程序。

5 导入准备就绪后，单击 《导入入口数据》按钮。

完成导入后，将显示 《入口数据导入结果》面板：



未完成的导入显示为红色。要对导入（或导出）问题查错，请查看应用程序服务器的系统控制台，或查看以下用户应用程序日志中的日志文件（如 jboss/server/IDM/log/server.log）的有关讯息：

```
com.novell.afw.portal.util
```

IV 入口小程序参照

以下章节说明如何配置 Identity Manager 用户界面中使用的身份入口小程序和系统入口小程序。

关于入口小程序 15

本章提供有关 Identity Manager 用户应用程序中使用的入口小程序的信息。包括以下主题：

有关管理入口小程序的更多信息，请参见第 9 章 "入口小程序管理"在第 165 页。

15.1 附属入口小程序

附属入口小程序提供了各种不同的功能，可以添加到 Identity Manager 用户应用程序中。附属入口小程序提供了电子邮件、文件系统和其它功能。有关更多信息，请参见：

入口小程序类别	详细信息
电子邮件	请参见 《Identity Manager 附属入口小程序管理指南》
文件系统	
杂项	

15.2 管理入口小程序

管理类别中的入口小程序用于控制用户界面的布局和内容。

注释：建议不要使用或修改这些入口小程序。它们为用户应用程序提供框架服务。

管理入口小程序包括：

入口小程序名称	说明
标题入口小程序	显示用户界面的标题信息和顶级选项卡控件。 此入口小程序没有自选设置。
共享页导航	显示包含 Identity Manager 用户应用程序共享页的菜单。 自选设置定义显示内容及显示方式。 请参见 "共享页导航入口小程序"在第 217 页 。

15.2.1 共享页导航入口小程序

共享页导航入口小程序生成与 Identity Manager 用户应用程序共享页的链接。自选设置可定义显示的共享页链接。自选设置包括：

自选设置	指定的内容
sharedpages-sorting	同一类别的共享页的显示顺序：升序 / 降序。
sharedpages-sortmode	共享页的排序方式：字母顺序或优先级顺序。
sharedpages-category	指定一个或多个共享页类别。
	类别名显示为标题，此类别中的所有共享页显示为链接。如果类别中不包含任何共享页，则不显示该类别。如果共享页不属于任何类别，则显示为未归类。
guest-category	指定希望在入口登录页中显示的入口小程序的类别。它必须是已存在的类别，且此类别中包含的页不得有任何 ACL 读取约束。

15.3 身份入口小程序

身份入口小程序用于 Identity Manager 用户应用程序的 《身份自助服务》选项卡。其中包括：

入口小程序名称	说明
创建	提供基于向导的界面，使用户可以在 Identity Vault 中创建对象。
	请参见第 16 章 "创建入口小程序参照" 在第 221 页 。
细节	使用户可以显示和处理实体的特性数据。
	请参见第 17 章 "细节入口小程序参照" 在第 227 页 。
组织结构图	使用户可以查看和浏览 Identity Vault 中对象之间的分级关系。
	请参见第 18 章 "组织结构图入口小程序参照" 在第 241 页 。
搜索列表	允许用户搜索 Identity Vault 中的对象。
	请参见第 20 章 "搜索列表入口小程序参照" 在第 269 页 。

15.4 口令入口小程序

口令入口小程序提供 Identity Manager 用户应用程序的口令自助服务功能。其中包括：

入口小程序名称	详细信息
IDM 询问应答	请参见第 19 章 "口令管理入口小程序参照" 在第 257 页
IDM 更改口令	
IDM 忘记口令	
IDM 提示定义	
IDM 登录	

15.5 系统入口小程序

系统入口小程序向 Identity Manager 用户应用程序提供服务。

注释 **:** 建议不要使用或修改此类别的入口小程序。

系统入口小程序包括：

入口小程序名称	说明
入口页控制器	显示用户当前通过共享页导航入口小程序选定的共享页。 此入口小程序没有自选设置。

创建入口小程序参照 16

本章说明如何使用 Identity Manager 用户应用程序中的创建入口小程序。包括以下主题：

16.1 关于创建入口小程序

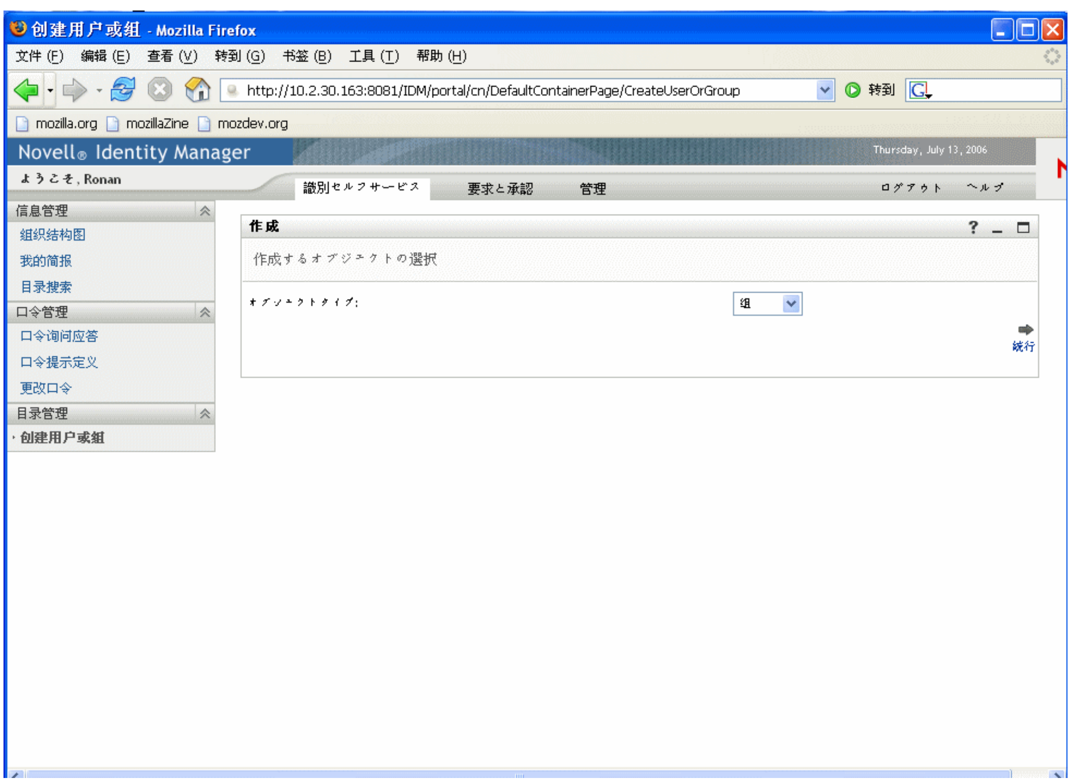
创建入口小程序提供易于使用的向导，用户可利用该向导创建各种类型的 Identity Vault 对象。入口小程序自选设置控制：

- 用户可以创建的对象类型。
- 用户可以提供的特性。

有关更多信息，请参见 "设置创建自选设置" 在第 224 页 。

创建入口小程序的默认配置 （通过 Identity Manager 用户应用程序的创建用户或组操作访问）允许用户创建用户、组或任务组。默认情况下，此入口小程序受用户应用程序管理员的限制。以下示例说明可通过默认的创建入口小程序向导执行的操作：

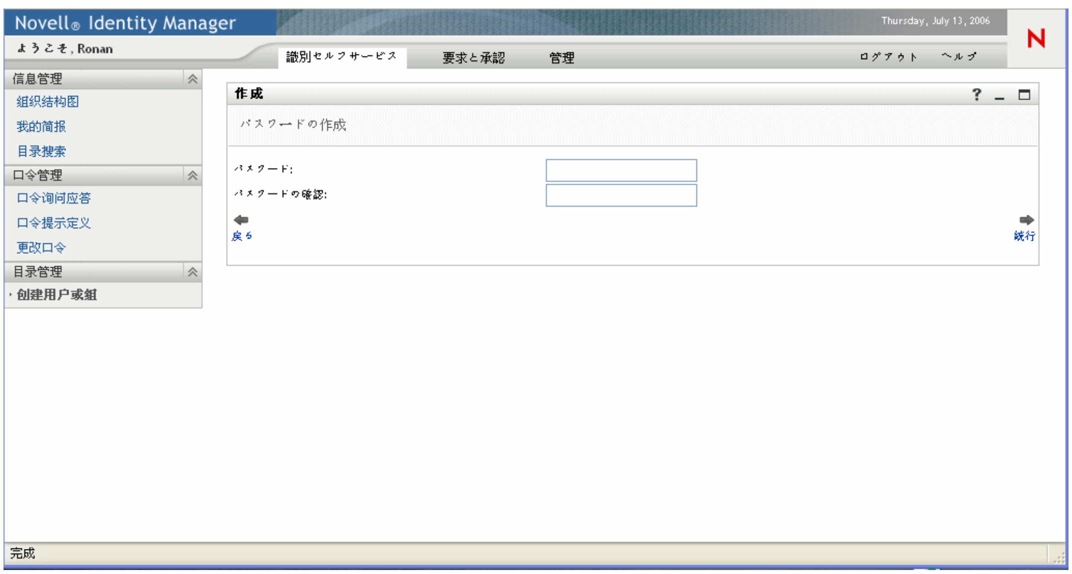
- 选择要创建的对象类型：



◆ 填充对象的特性：



◆ 对象类型需要时，提示输入口令：



如果指派了口令策略，此入口小程序将显示所有自定义策略讯息。

◆ 成功创建对象后，将提供一条信息性讯息，此讯息将链接到该对象的细节入口小程序（假设已同样配置了细节入口小程序），以供进一步编辑。

16.2 配置创建入口小程序

要配置创建入口小程序，需要：

步骤	任务	说明
1	确定默认的创建用户或组功能是否满足要求	如果满足要求，则无需再执行任何操作。 如果不满足要求，则需要完成其余步骤。
2	定义允许用户创建的对象类型	将对象和特性添加到目录提取层。 有关更多信息，请参见第 4 章 “配置目录提取层”在第 69 页 。
3	决定希望用户访问新入口小程序的方式	希望用户从现有页还是从新页面起动此入口小程序？哪些用户可以访问此入口小程序和页？ 有关页的更多信息，请参见第 7 章 “页管理”在第 125 页 。
4	指定可以访问此页和入口小程序实例的用户	编辑页的安全性并将用户添加到列表中。有关限制用户访问页的更多信息，请参见第 7 章 “页管理”在第 125 页 。 编辑入口小程序实例以更改安全性。有关限制用户访问入口小程序的更多信息，请参见第 9 章 “入口小程序管理”在第 165 页 。
5	设置入口小程序的自选设置	可使用自选设置定义： ◆ 用户可以创建的对象。 ◆ 创建过程中需提供的特性。 有关更多信息，请参见“设置创建自选设置”在第 224 页 。
6	测试	验证对象已创建且已正确填充特性。
7	在 eDirectory 中为终端用户建立适当、有效的权限	要创建对象，用户需要成为创建对象的组织单位和组织中的**受托者**。

16.2.1 目录提取层设置

必须在目录提取层中按以下方式定义创建入口小程序的用户可以创建的对象和可以填充的特性：

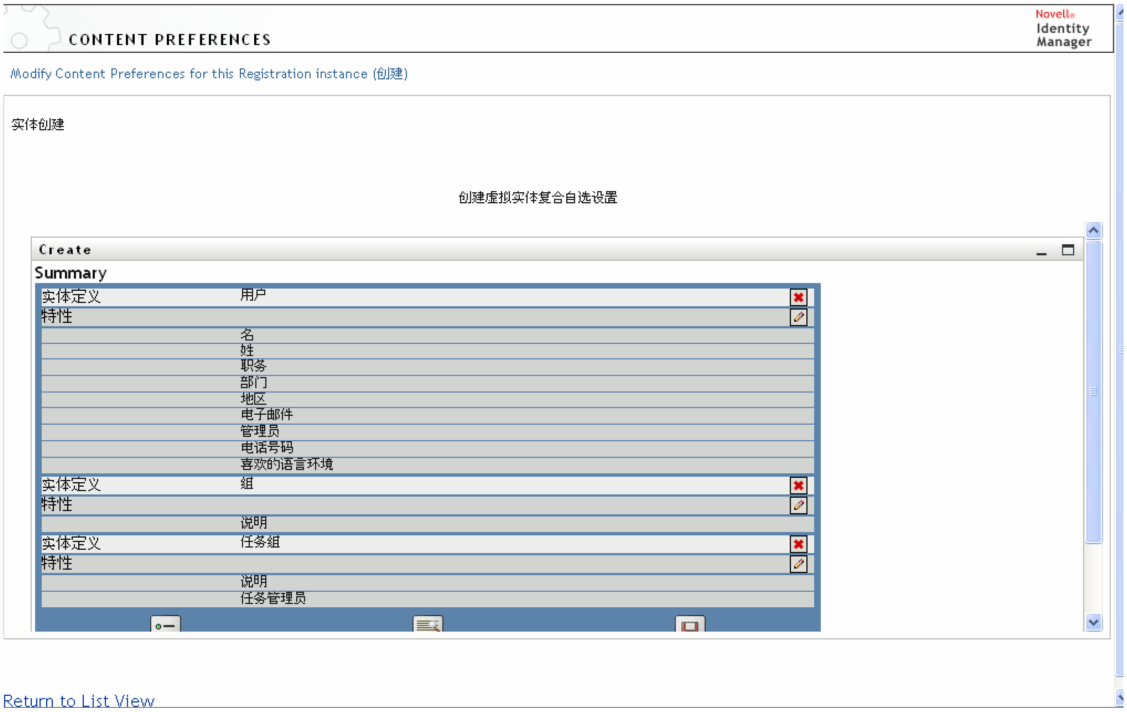
定义类型	属性	值
实体	创建	选中
	查看	选中 如果未选中，该实体将不显示在可以创建的实体列表中。
	用于创建的树枝	指定有效的 Identity Vault 树枝。 如果未提供有效的树枝，则使用在安装用户应用程序时指定的根树枝。
	口令	如果实体类型在创建时需要口令，则选中。 可以访问创建并具有 OU 受托者权限的任何人都可以创建用户并指派**起始口令**。新用户首次登录时，会被重定向到 IDM 更改口令入口小程序，用户可以在此修改起始口令。 有关 IDM 更改口令入口小程序的更多信息，请参见第 19 章 “口令管理入口小程序参照” 在第 257 页 。
特性	已启用	选中
	可读的	如果未选中 《已启用》 或 《可读的》 (False)，此入口小程序将无法使用此特性。

有关设置提取层的更多信息，请参见第 4 章 “配置目录提取层” 在第 69 页 。

16.3 设置创建自选设置

可以配置允许用户创建的对象类型，以及允许或需要由设置自选设置提供的特性。

创建入口小程序的自选设置包含在单独的自定义自选设置页中。打开此页，将显示单独的创建自选设置：



下面介绍这些自选设置 （或单击 《说明》按钮显示此入口小程序的联机帮助）。

自选设置	说明
实体定义	要创建的对象类型名称。 表示实体定义块的开头，可以在该实体定义块中定义入口小程序将如何处理创建操作。 **要限制对象，请执行以下操作：** 复合自选设置中列出的对象显示在下拉列表中。要限制用户可以创建的对象，请通过 《删除》按钮从此自选设置表中将其去除。 **要添加其它实体，请执行以下操作：** 单击 《添加实体定义》，然后完成向导。

自选设置	说明
特性	控制提示用户填充的特性。必须包括对象的所有必需特性，否则对象的实际创建将失败。此外，如果丢失了某个必需特性，则不能正确保存自选设置。 **要添加或去除特性，请执行以下操作：** ◆ 单击 《修改特性》按钮。  ◆ 要添加特性，请从可用特性列表中选择。可以使用 Ctrl 键或 Shift 键选择多个特性。 ◆ 单击箭头，将其移动到 《选定》列表中。执行相反的操作可以去除特性。 ◆ 要对特性列表重新排序，请单击 《选定》列表右侧的向上箭头和向下箭头。单击 《提交》。 **特性和数据类型：** 特性的数据类型可以影响它的显示方式。例如，如果将特性定义为本地或全局列表子类型，则特性显示在列表框中。 有关更多信息，请参见 "使用实体和特性"在第 79 页 。

完成自选设置面板 要验证已提交的有效项，请单击 《提交》。如果某项无效，自选设置页的顶部会显示一条错误讯息。可以单击 《提交》且没有错误时，单击 《返回到列表视图》。返回到列表视图后，必须单击 《保存自选设置》。

细节入口小程序参照 17

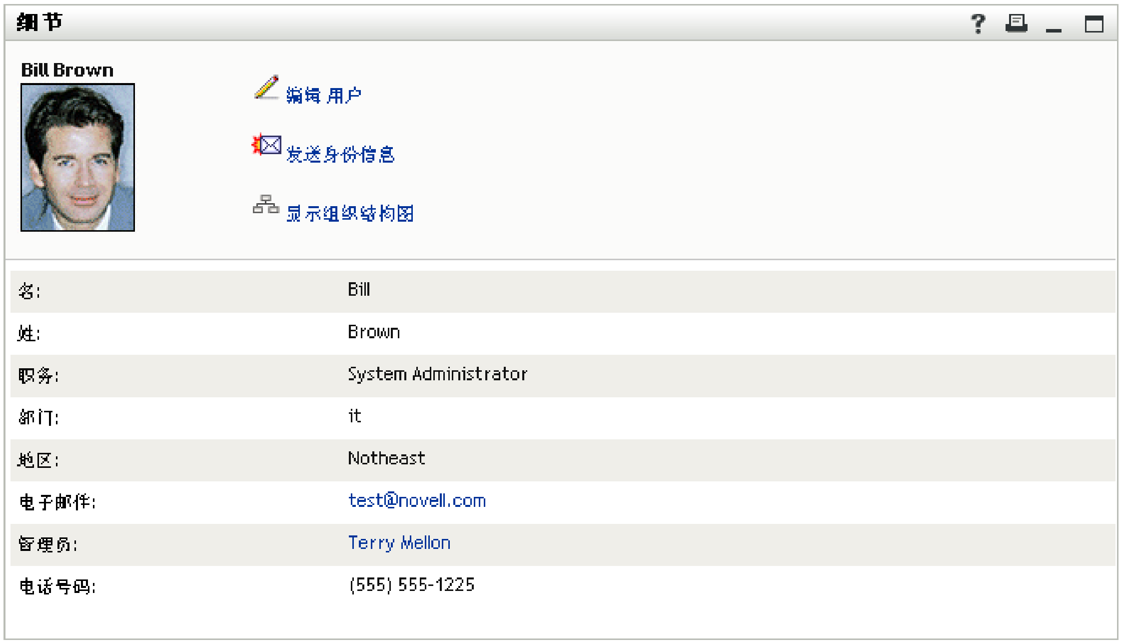
本章说明有关细节入口小程序的内容，用户可以在细节入口小程序中显示和处理实体的特性数据。它是 Identity Manager 用户应用程序 《身份自助服务》选项卡中的 《我的简报》操作的基础。包括以下主题：

17.1 关于细节入口小程序

细节入口小程序为用户提供了实体的特性及特性值的细节视图。入口小程序有以下两种模式：显示模式和编辑模式。访问细节入口小程序时，用户可以利用其内置功能处理这些信息，这些功能包括：

17.1.1 显示实体数据

访问细节入口小程序时，将显示选定实体，如用户或组的特性数据。例如，下面是用户 Bill Brown 查看自己的信息时，细节入口小程序可能显示的内容：



用户图像 默认情况下，细节入口小程序的配置包括 User Photo 特性。但如果 Identity Vault 中不包括此特性或未填充此特性，运行时会显示默认图像。如果将用户图像储存在其它位置，可以通过配置入口小程序来显示它们。

有关更多信息，请参见 “动态装载图像” 在第 231 页 。

确定要显示的特性

细节入口小程序仅显示以下特性：

- 目录提取层数据定义提供用于查看的特性

  有关 VDD 配置的更多信息，请参见第 4 章 “配置目录提取层” 在第 69 页 。
- 在细节自选设置中指定的特性

  要了解细节入口小程序中指定将显示的特性，请参见 “设置自选设置” 在第 238 页 。
- 当前用户具有查看权限的特性

  例如，对薪水特性有权限的经理将看到这些数据，但其他用户看不到。

  有关更多信息，请参见 “指派实体权限” 在第 235 页 。
- 当前由值填充的特性

确定特性的显示方式

显示特性时，细节入口小程序会将数据格式设置为文本，但以下情况除外：

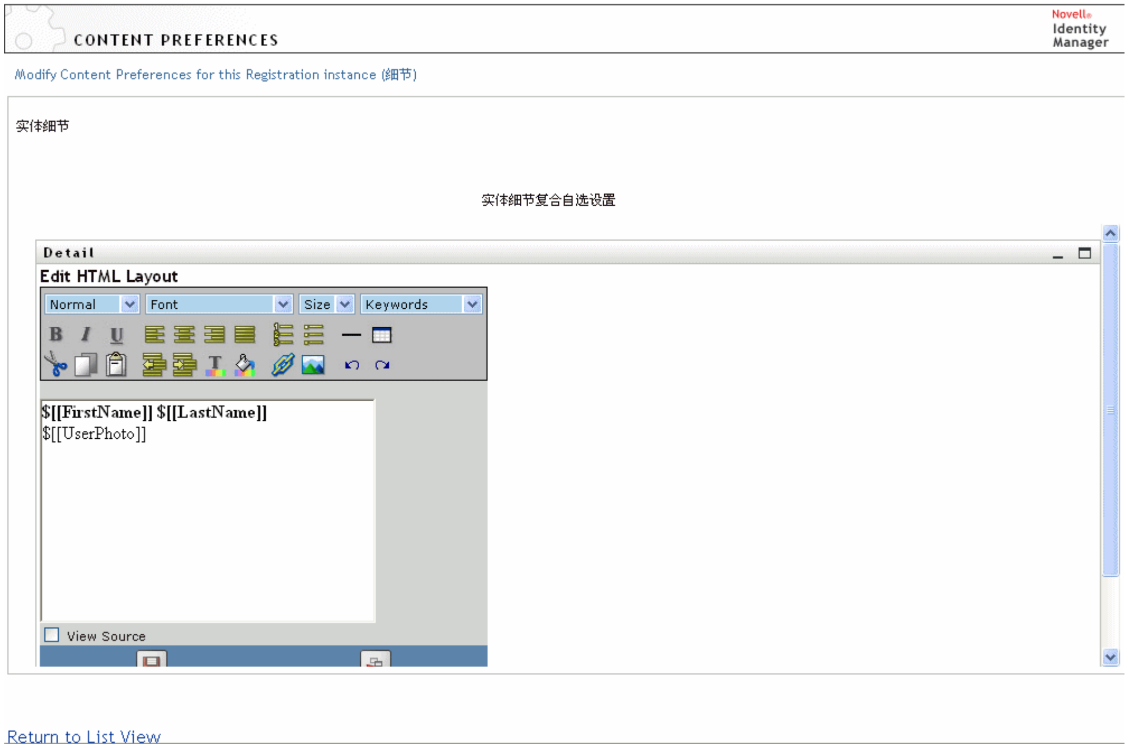
提取层定义中的格式规格	显示方式
格式：电子邮件	作为 mail-to 链接
格式： ◆ GroupWise-IM ◆ AOL-IM ◆ Yahoo-IM	作为启动交谈和添加该用户的图标
数据类型：二进制 格式：图像	作为查看图像的按钮和链接
数据类型：布尔值	作为指示 True 或 False 的已禁用单项选择按钮 这些按钮在显示时未指示默认值，这是因为在用户指定值之前，不会实际创建此特性。
多值：选中	作为可重复使用的编辑、添加和去除单个特性值的控件集（以逗号分隔列表的形式）
控制类型：DNLookup	作为链接 在上述示例中，显示链接 (Terry Mellon) 以访问 Bill Brown 的经理的细节数据。
控制类型： ◆ 本地列表 ◆ 全局列表	作为显示标签，而不是实际 （键）值 例如， EmployeeType 特性显示为 Full Time，而不是实际值 ft。

确定标题区域显示的内容

可以使用标准 HTML 功能对细节入口小程序的标题区域进行布局：



细节自选设置提供了 *HTML* 布局编辑器，可以使用该编辑器创建所需的外观和内容：



使用 HTML 布局编辑器

HTML 布局编辑器提供了 HTML 编辑器的典型功能，可用于定义文本格式和列表，指定锚和图像等。

关键字 设计布局时，可以使用 《关键字》下拉菜单在细节入口小程序的标题区域插入变量，运行时可用特定特性值替换这些变量。也可以使用以下语法键入关键字：

```
$[[keyword]]
```

其中，关键字为特性值 （如 LastName）。

可以使用以下语法来连结特性：

```
$[[keyword+keyword]]
```

例如：

```
$[[FirstName+LastName]]
```

可以根据需要连结多个特性，也可以包括引号中的字符串，如下所示：

```
$[[keyword+”sample text”+keyword]]
```

将显示关键字的值和引号中的文本。

注释 **:** 在布局中错误键入关键字时，运行时将显示为其原来的样式 （包括 $[[]]）。

动态装载图像 若要显示储存在 Identity Vault 中的图像 （如用户照片），可以使用 HTML 布局编辑器添加此特性名称。例如，添加 User Photo 特性可以显示用户的照片。如果图像储存在 Identity Vault 以外，则需要在 HTML 编辑器中的 《查看来源》方式下使用 IMG: 标签，方法如下所示：

1. 转至入口小程序的自选设置，访问 HTML 编辑器。
2. 单击 《查看来源》。
3. 使用 IMG: 标签按照如下语法将位置、特性键和文件扩展名组合在一起：

   ```
   $[[IMG:”URL” + attribute-key-name + ”fileextension”]]
   ```

如果已按姓氏将员工照片储存为 JPG 图像，并且放在应用程序服务器的 /images 子目录中，则要使用以下示例中的语法：

```
$[[IMG:"http://myhost:8080/images/"+LastName+".jpg"]]
```

在运行时，入口小程序会将 URL 与 LastName 特性及文件扩展名 .jpg 连结在一起。

请注意， HTML 编辑器支持灵活的语法。它支持文本和特性的任意组合，语法如下：

```
$[[IMG:”some text” + attribute-key-name + ...]]
```

17.1.2 编辑实体数据

细节入口小程序自动提供编辑链接 （如 《编辑您的信息》、《编辑用户》或 《编辑设备》），以便从显示模式切换到编辑模式。这样用户就对当前实体具有适当的权限，可以更改其特性值并保存这些更改。

例如，以下是用户 Bill Brown （具有所需的权限）编辑自己的信息时细节入口小程序可能显示的内容：



注释：对于布尔特性，如果两个单项选择按钮都未选中，则表示用户不具有该特性。选中 *True* 或 *False* 单项选择按钮，可以同时为用户创建此特性并设置值。

确定要显示的特性

在编辑模式下，细节入口小程序仅显示以下特性：

- 目录提取层数据定义提供用于查看的特性

  有关数据定义的更多信息，请参见第 4 章 “配置目录提取层” 在第 69 页。
- 当前用户具有查看权限的特性

  例如，对薪水特性有权限的经理将看到这些数据，但其他用户看不到。

  有关更多信息，请参见“指派实体权限” 在第 235 页。

特性必须满足上述所有准则，才能在编辑模式中显示。

确定特性的显示方式

在编辑模式下，细节入口小程序将每个可编辑的特性格式化为文本框，但以下情况除外：

特性类型规格 （在 VDD 文件中）	显示方式
数据类型：二进制 格式：图像	作为实体图像上载入口小程序的按钮和链接，用于查看、更新或添加图像
数据类型：布尔值	作为指示 True 或 False 的单项选择按钮
隐藏：选中	作为标为 《隐藏》的复选框
多值 = 选中	作为控件集，用于编辑、添加和去除特性值
控制类型：DNLookup	作为起动参数列表入口小程序的按钮，用于搜索和选择 DN
控制类型： ◆ 本地列表 ◆ 全局列表	作为下拉列表 （如果可用，允许多项选择）

无法编辑的特性 （由于定义或由于用户权限不足）将显示为禁用或只读。

验证更改

在编辑期间，将自动执行以下特性类型规范的数据验证：

- 格式：电子邮件
- 数据类型：整数
- 控制类型：范围

使用本地列表或全局列表控制类型时，显示的列表中可能包括特性指定界限以外的值。但这些值将被标记为超出范围，验证将阻止其提交。

定义默认的我的简报实体

在目录提取层定义实体时，可以指定默认的我的简报实体的值 （在目录提取层编辑器的 Configuration 要素中），以指定用于编辑的其它实体定义。从显示模式切换到编辑模式时，细节入口小程序始终检查是否已指定此要素，然后使用适当的实体定义显示特性。

例如，假定学生的实体定义包括作为默认的我的简报实体值的用户。在这种情况下，显示模式将使用学生实体定义，但编辑模式将使用用户实体定义。

17.1.3 通过电子邮件发送实体数据

细节入口小程序自动提供名为 《发送身份信息》的链接。用户可以单击它，将当前实体 《细节》的 URL 通过电子邮件发送至一个或多个用户。通过电子邮件发送细节 URL （而不是实际信息），可以维护安全性 （因为任何收到此 URL 的人都需要适当授权才能使用它）。

17.1.4 组织结构图链接

细节入口小程序自动提供名为 《显示组织结构图》的链接。用户可以单击它，以显示当前实体的组织结构图入口小程序。

例如，如果要查看用户 Bill Brown 的 《细节》，单击此链接将显示：



有关组织结构图入口小程序的更多信息，请参见第 18 章 “组织结构图入口小程序参照”在第 241 页 。

17.1.5 其它实体细节的链接

配置细节入口小程序时，可能希望用户能够从当前实体链接到相关实体。将使用控制类型 *DNLookup* 在目录提取层中定义的特性包括在内即可实现。

如果 Manager 特性显示在用户的 《细节》中，将显示为链接。单击该链接将显示该用户的经理的 《细节》。



有关目录提取层的更多信息，请参见第 4 章 “配置目录提取层”在第 69 页 。

要了解细节入口小程序中显示哪些特性，请参见 “设置自选设置”在第 238 页 。

17.1.6 打印实体数据

默认情况下，细节入口小程序的显示设置会在入口小程序的标题栏上启用 《打印》选项。如果启用 《打印》，用户可以单击它，以显示细节内容的打印机友好版本：

若要更改细节入口小程序的此项设置或其它设置，请使用 《管理》选项卡更新 *DetailPortlet* 的入口小程序注册 （在 《入口小程序管理》页上）。

有关更多信息，请参见第 9 章 “入口小程序管理”在第 165 页 。

17.2 前提条件

开始使用细节入口小程序之前，需要了解以下内容：

- “配置目录提取层”在第 235 页
- “指派实体权限”在第 235 页

17.2.1 配置目录提取层

细节入口小程序在很多方面都取决于目录提取层定义。本章的以下各节提供了有关如何配置目录提取层数据定义，以支持细节入口小程序的特定功能的指导：

- “显示实体数据”在第 228 页
- “编辑实体数据”在第 231 页
- “使用页中的细节”在第 237 页

有关配置的更多信息，请参见第 4 章 “配置目录提取层”在第 69 页 。

17.2.2 指派实体权限

用户若要在细节入口小程序中访问实体及其特性，必须在 *eDirectory* 中为其指派相应的权限：

要执行的操作	**用户需要的权限**
显示特性	读
编辑特性	写

通过将用户指定为对象 （实体）的受托者为其指派权限。然后可以指定要为哪些特性指派哪些权限。

17.3 从其它入口小程序起动细节入口小程序

起动细节入口小程序的常用方法是在其它身份入口小程序中选择实体后将其启动。可以通过以下方式起动细节入口小程序：

- “从搜索列表入口小程序起动”在第 236 页
- “从组织结构图入口小程序起动”在第 237 页

17.3.1 从搜索列表入口小程序起动

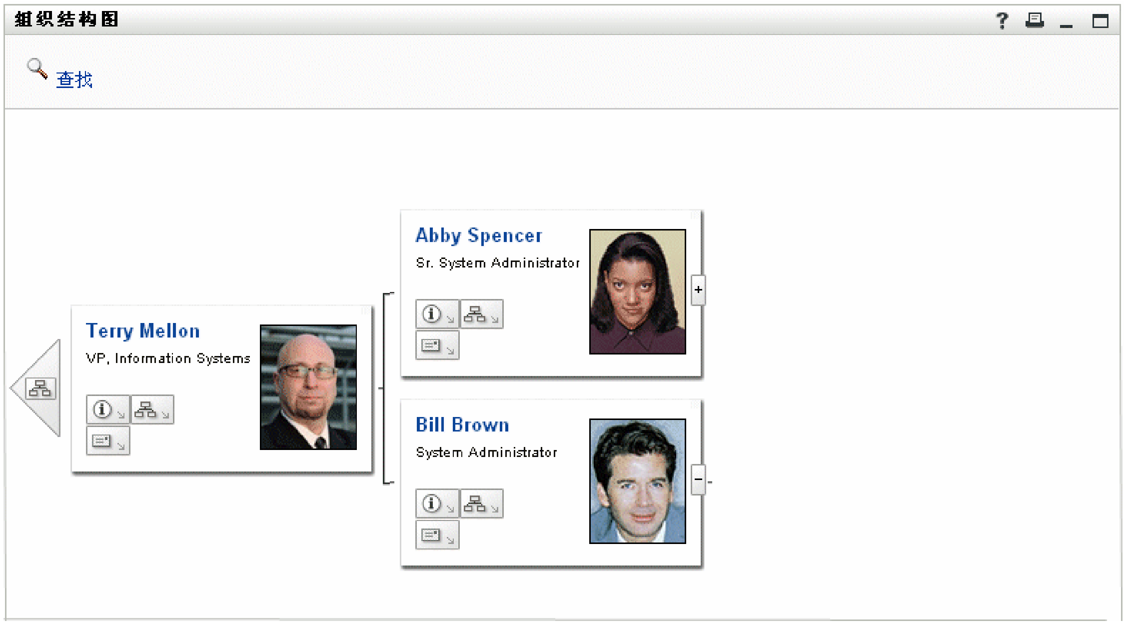
在搜索列表入口小程序中，用户可以在搜索结果中单击实体行以显示该实体的细节。例如，单击以下列表中的 Bill Brown 行将显示包含其特性数据的细节入口小程序：



有关搜索列表入口小程序的更多信息，请参见第 20 章 “搜索列表入口小程序参照”在第 269 页 。

17.3.2 从组织结构图入口小程序起动

在组织结构图入口小程序中，用户可以单击实体的 《身份操作》图标，然后选择 《显示信息》，以显示该实体的细节。例如，在以下组织结构图中单击 Bill Brown 的 《显示信息》，将显示包含其特性数据的细节入口小程序：



有关组织结构图入口小程序的更多信息，请参见第 18 章 “组织结构图入口小程序参照” 在第 241 页 。

17.4 使用页中的细节

如果要为用户提供自助服务，使其可以显示并可能编辑自己的特性数据，则可以将细节入口小程序添加到共享页中。在共享页中使用细节入口小程序时，它将自动访问当前用户 （或其它默认实体）的数据。

例如，用户 Bill Brown 可以登录并通过细节入口小程序转至以下个人页以维护自己的信息：



要确定细节入口小程序在本方案中使用的实体定义 （通过页访问此细节入口小程序，而不是通过其它入口小程序起动），可在目录提取层的 Configuration 要素中指定默认的晕业募虮尸实体设置。

17.5 设置自选设置

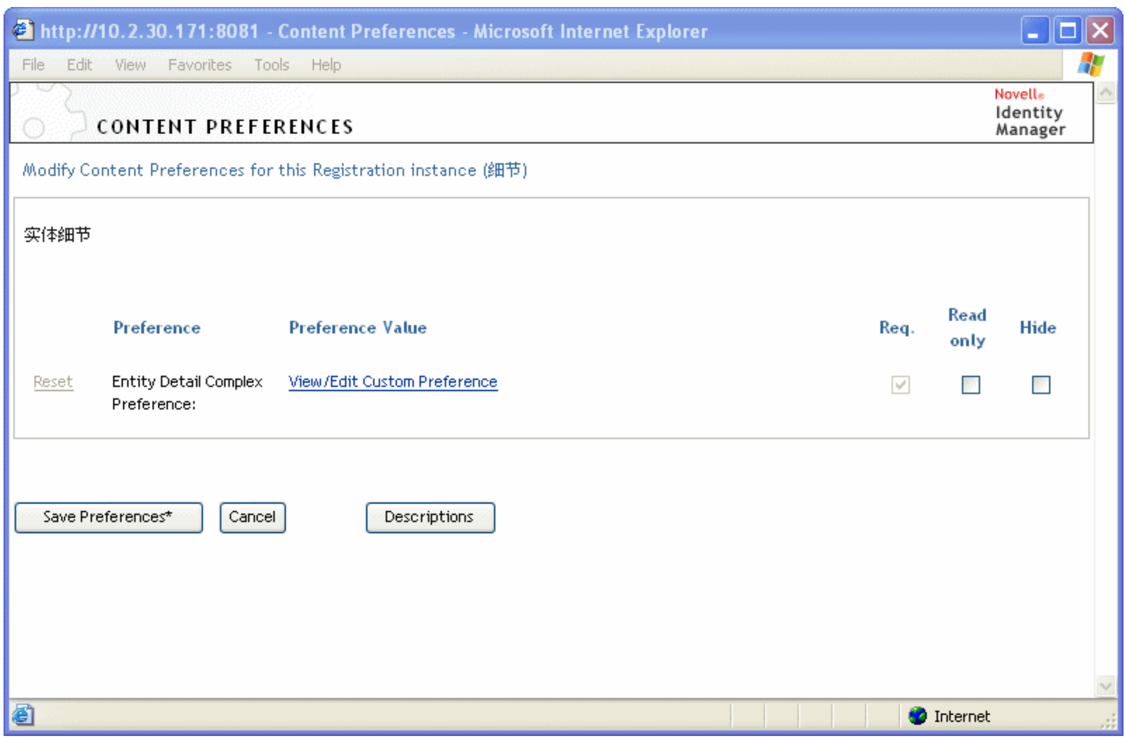
设置自选设置可以定义细节入口小程序的内容和外观。使用细节入口小程序的方式将决定设置其自选设置的位置：

要了解从共享页或树枝页访问入口小程序自选设置的有关内容，请参见第 7 章 “页管理” 在第 125 页 。

要了解访问入口小程序注册的入口小程序自选设置的有关内容，请参见第 9 章 “入口小程序管理” 在第 165 页 。

17.5.1 关于自选设置

细节自选设置全部包含在单独的细节复合自选设置中：



打开此复合自选设置后，将显示单独的细节自选设置：



这些自选设置仅适用于显示模式（非编辑模式）。其中包括：

自选设置	细节
实体定义	指定细节入口小程序用于特定实体类型（如用户、设备或组）时要显示的特性列表和 HTML 布局。 可以单击 《添加实体定义》以指定对附加实体类型的细节支持。
显示为列表的特性	指定希望入口小程序显示所选实体的哪些特性。这些特性将按所选顺序列出。 将提供一个按钮，以便根据需要添加或去除特性。
HTML 布局	提供的按钮可打开 **HTML 布局编辑器**，在此编辑器中可以设计细节入口小程序将显示的所选实体的标题区域。 有关详情，请参见 “确定标题区域显示的内容”在第 229 页 。

组织结构图入口小程序参照 18

本章说明如何修改现有组织结构图功能或将新的组织结构图功能添加到 Identity Manager 用户应用程序。包括以下主题：

- "关于组织结构图" 在第 241 页
- "配置组织结构图入口小程序" 在第 243 页
- "设置组织结构图自选设置" 在第 244 页

18.1 关于组织结构图

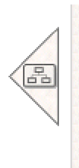
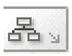
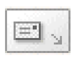
组织结构图入口小程序允许终端用户查看和浏览 Identity Vault 中对象之间分级关系的图形表示形式。例如，可以定义显示以下层次关系的组织结构图入口小程序：

- 组织 （如员工和经理）
- 组的成员资格 （如组中的所有员工）
- 指派给用户的设备 （如手机和便携式计算机）

Identity Manager 用户应用程序 《身份自助服务》选项卡的默认配置包括组织结构图操作。此操作是一个为显示 Identity Vault 中用户对象之间的关系而配置的组织结构图入口小程序。以下示例说明默认组织结构图入口小程序如何显示此关系 （使用样本数据）。



内置链接 组织结构图入口小程序包括以下内置链接。

链接	说明
	允许用户导航至下一上级。只有在查看父实体与子实体相同的关系时此链接才可用。
	起动细节入口小程序。 可通过组织结构图布局自选设置来配置此内置链接，详见 “组织结构图布局自选设置” 在第 249 页
	显示组织结构图列表。允许用户选择要查看的组织结构图。 此组织结构图列表是动态的。它显示共享同一父实体类型的其它组织结构图。例如，如果在查看经理 / 员工组织结构图 （父实体是用户）时单击此图标，则查看到的组织结构图列表将仅包含父实体也是用户的关系。 可通过组织结构图布局自选设置来配置此内置链接，详见 “组织结构图布局自选设置” 在第 249 页
	起动电子邮件工具以进行以下操作： ◆ 发送当前所选用户的身份细节 ◆ 撰写电子邮件 可通过组织结构图布局自选设置来配置此内置链接，详见 “组织结构图布局自选设置” 在第 249 页
	《查找》链接允许用户执行实体搜索。搜索使得找到的实体成为所显示图表的顶部节点。
	允许用户向下钻取到下一级别。

有关在组织结构图中添加和限制内置链接的更多信息，请参见 “组织结构图布局自选设置” 在第 249 页 。

18.1.1 关于组织结构图关系

组织结构图入口小程序显示目录提取层中定义的关系。安装 Identity Manager 用户应用程序后可以使用以下关系。

- 组成员资格
- 经理 - 员工
- 用户组

要了解有关创建或修改组织结构图关系的更多信息，请参见第 4 章 “配置目录提取层” 在第 69 页 。

注释 **:** 组织结构图入口小程序不完全支持动态组。无法将动态组定义为关系中的父实体，但是可以将其定义为关系中的子实体。

18.1.2 关于组织结构图显示

默认情况下，组织结构图显示在某一区域的入口小程序的框架中，该区域由 《入口小程序宽度》和 《入口小程序高度》自选设置来定义。如果内容所需的区域超过定义的区域，则入口小程序的边界会扩展，而页面的高度和宽度也会扩展。用户可以通过单击入口小程序标题栏上的最大化图标来完全显示组织结构图。 （默认情况下，从细节入口小程序起动时，组织结构图以完全最大化模式显示。）

用户图像 默认情况下，用户对象的组织结构图布局包括 User Photo 特性。但是，如果 Identity Vault 中不包括或未填充此特性，则组织结构图在运行时会忽略此特性。如果照片储存在不同位置，则可以配置组织结构图以显示那些照片。

有关更多信息，请参见 “动态装载图像”在第 254 页 。

18.2 配置组织结构图入口小程序

要配置组织结构图入口小程序，需执行以下任务：

步骤	任务	说明
1	定义要显示的关系	可以使用与 Identity Manager 用户应用程序一起安装的某个预定义关系，或创建自己的关系。 有关定义关系的更多信息，请参见第 4 章 “配置目录提取层”在第 69 页 。
2	验证目录提取层中是否提供要在关系中使用的实体和特性	有关定义关系的更多信息，请参见 “目录提取层设置”在第 243 页 。
3	确定要显示此关系的位置	是希望新建一个页来起动组织结构图，还是希望从细节入口小程序或从其它组织结构图起动该组织结构图？ 有关创建页和向这些页中添加入口小程序的更多信息，请参见第 7 章 “页管理”在第 125 页 。
4	设置入口小程序的自选设置	可使用自选设置定义： ◆ 要显示的特性 ◆ 显示特性的方式 （特性的 HTML 布局） 有关更多信息，请参见 “设置组织结构图自选设置” 在第 244 页 。
5	测试	测试关系定义和布局
6	设置 eDirectory 权限并建立增强性能所需的所有索引	**有效权限** - 要显示由入口小程序定义的特性，用户对这些特性必须拥有**读**权限。 **性能增强** - 由于关系的子特性用于执行 LDAP 搜索，因此可以通过向该子特性添加 eDitectory 值索引来增强组织结构图的显示性能。

18.2.1 目录提取层设置

必须在目录提取层中定义显示在组织结构图内的实体和特性。下表显示了必须为显示在组织结构图内的每个实体和特性设置的特性和属性。

定义类型	设置	值
实体	查看	选中 (True)
特性	读	选中 (True)
	搜索	选中 (True)

《查找》链接要求《查找》链接允许用户通过搜索与父实体关键字类型相同的其它对象来定位组织结构图。它要求父实体关键字至少有一个特性的 《要求》和 《搜索》访问属性设置为 True （在目录提取层编辑器中选中）。如未设置，则不能填充 《查找》链接的 《对象查找》对话框，因此将显示为空对话框。

有关实体和特性配置的更多信息，请参见第 4 章 “配置目录提取层”在第 69 页 。

18.2.2 设置组织结构图自选设置

可以定义两种类型的自选设置：

- “组织结构图关系自选设置”在第 245 页
- “组织结构图布局自选设置”在第 249 页

组织结构图关系自选设置

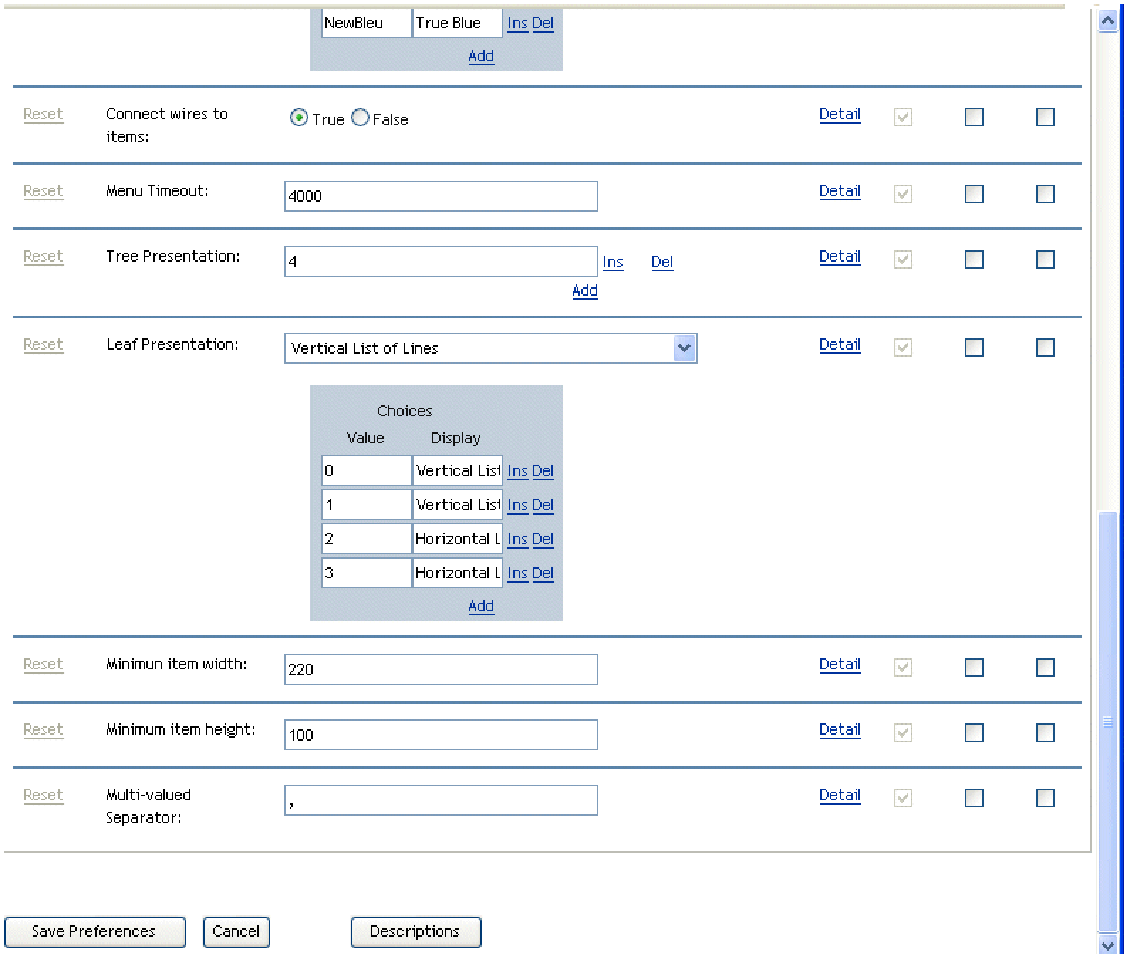
组织结构图关系自选设置包括在一个自选设置页中。



.

.

.



自选设置	操作
显示布局	单击《查看 / 编辑自定义自选设置》以访问布局自选设置。这些内容在 “组织结构图布局自选设置”在第 249 页 中有所介绍。
关联关键字	键入关联关键字。此值必须对应于目录提取层中指定的某个关联关键字。

自选设置	操作

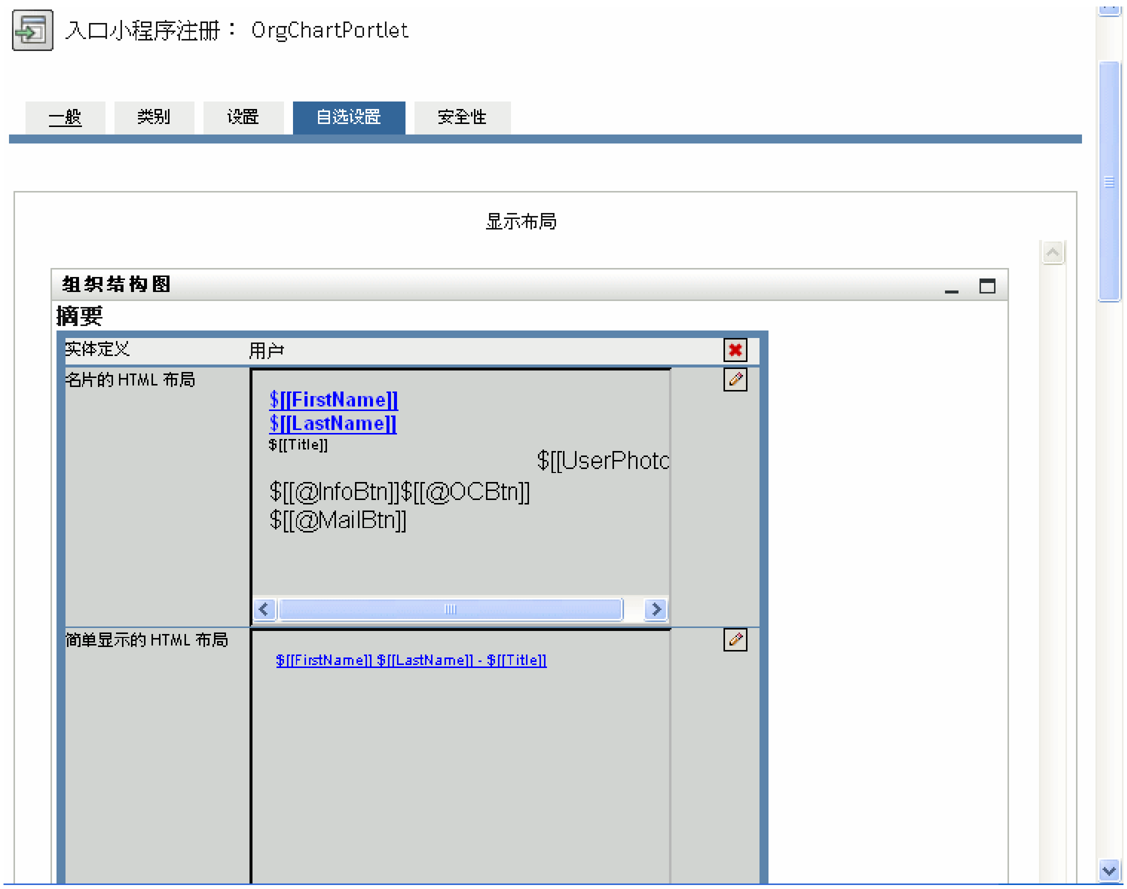
父实体关键字	键入实体 （表示要显示的组织结构图的根节点）的 DN 或键入 ${User/id} 以显示当前用户的组织结构图。 （${User/id} 参数解析到当前用户的 DN。）
	
	该值不得超出目录提取层中 search-root 属性所指定的节点，否则将导致 LDAP 搜索失败。
	
	以下是有效 DN 的一些示例 （使用样本数据）：
	
	◆ 要显示 user2users 关联关键字且以名为 Jack Miller 的员工为组织结构图的根节点，则必须指定：
	
	`cn=jmiller,ou=users,ou=sample,o=novell`
	
	◆ 要显示 group2users 关联关键字且以会计组为根节点，则必须指定：
	
	`cn=Accounting,ou=groups,ou=sample,o=novell`

默认深度	指定首次显示组织结构图的深度。 ◆ 0 - 仅显示根 ◆ 1 - 显示根及其子级 ◆ 2 - 显示根、子级和孙级 依此类推。如果此值递增到大于 《最大深度》（见下文），则 《最大深度》值优先。
最大深度	定义用户在组织结构图中能向下钻取的最大深度。这与浏览受有效权限限制的组织结构图的能力不同。
OrgChart 外观	名片 eGuide Novell.com 连线 纯蓝
对项目进行连线	指定是否用连线连接组织结构图卡。False 意味着不连接。
菜单超时	当前显示菜单 （对于内置链接）消失前的毫秒数。

自选设置	操作
树显示	定义 OrgChart 的排列方向、分布状态以及每个深度级别的外观。 开头的 *n* 个值将定义排列方向、分布状态和从 0 到 *n-1* 级别的外观。最后一个值将反复用于深度大于 *n-1* 的级别。值必须在 0 到 5 之间。 值为： 0: 将名片置于项的垂直列表上方 1: 在项的垂直列表上方连线 2: 将名片置于项的水平列表上方 3: 在项的水平列表上方连线 4: 将名片置于项的垂直列表之前 5: 在项的垂直列表之前连线
树叶显示	定义 OrgChart 的排列方向、分布状态以及单个 OrgChart 分支最大深度的外观
最小项目宽度	此值应等于 round('item min height' * 1.618)
最小项目高度	此值应等于 round('item min width' / 1.618)
用于多值特性的分隔符	用作多值特性的分隔符的字符。

组织结构图布局自选设置

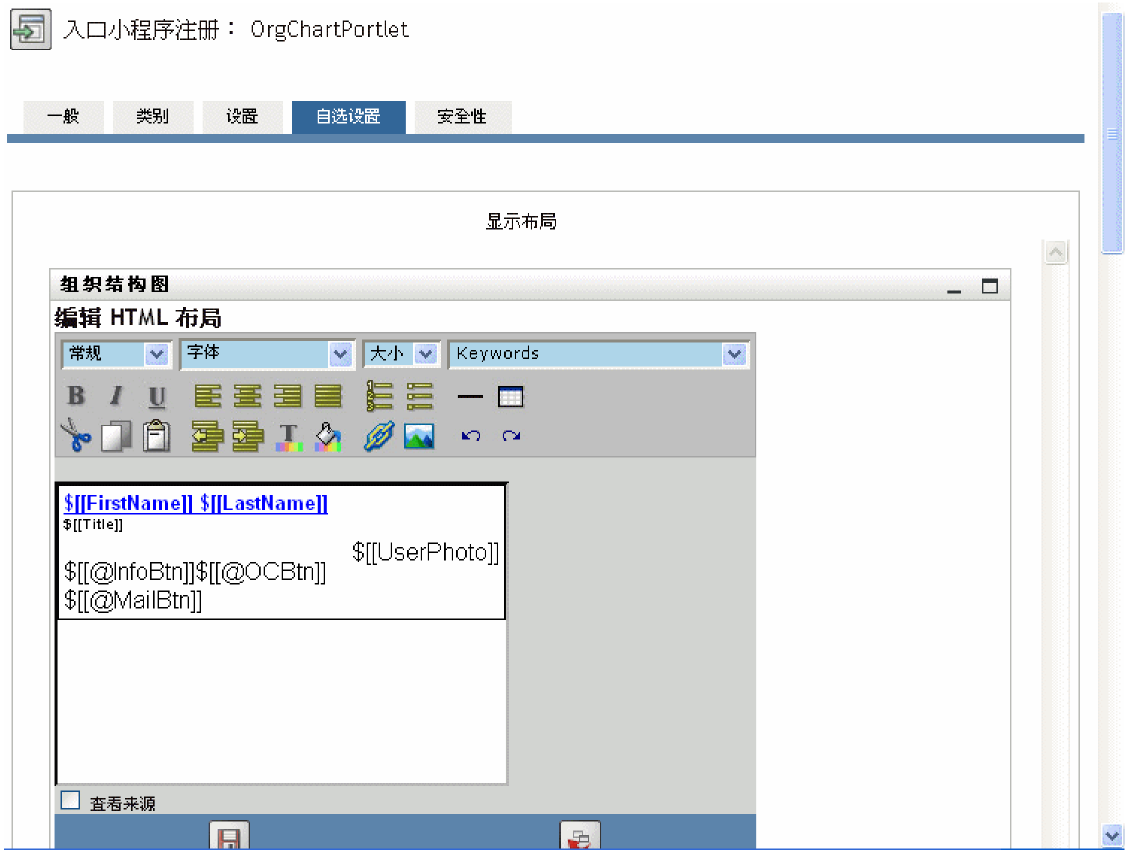
使用组织结构图布局自选设置可以定义组织结构图项的 HTML 显示布局。可以使用所选的 HTML 编辑器来进行更准确地编辑。请参见“使用外部编辑器”在第 254 页。



名片的 *HTML* 布局 - 默认布局。

用于简单显示的 *HTML* 布局 - 树显示自选设置设置为 1 时所显示的布局。

HTML 编辑器 单击《编辑》按钮可访问 HTML 编辑器。HTML 编辑器如下所示：



使用 HTML 编辑器

HTML 编辑器提供了用于定义组织结构图的叶布局的 WYSIWYG 界面。它提供了 HTML 编辑器的常用功能，可定义文本格式和列表，以及指定定位点和图像等。使用 《关键字》下拉列表可在布局区域内放置特性、命令和导航 URL。从下拉列表中选择关键字时，此关键字会以合适的语法插入，但是也可以在布局区域内添加 HTML。

关键字 设计布局时，可以使用 《关键字》下拉列表来插入变量，在运行时会用特定特性值来代替这些变量。或者使用以下语法来键入它们的参照：

```
$[[keyword]]
```

其中关键字是实体特性的值，如 LastName。

可以使用以下语法来连结特性：

```
$[[keyword+keyword]]
```

例如：

```
$[[FirstName+LastName]]
```

可以根据需要连结多个特性，也可以包括引号中的字符串，如下所示：

```
$[[keyword+"sample text"+keyword]]
```

将显示关键字的值和引号中的文本。

注释 **:** 如果布局中关键字键入有误，则它将在组织结构图中按原样显示 （包括 $[[]]）。

HTML 编辑器功能和关键字用法 要使用 HTML 编辑器功能和 《关键字》下拉列表，请执行以下操作：

功能	提示
《插入链接》按钮	要插入链接，请执行以下操作： **在 Mozilla 中：** 1. 突出显示要超级链接的文本并单击 《插入链接》。 2. 键入 URL 并单击 《创建链接》。 3. 保存自选设置。 **在 IE 中：** 1. 单击 《插入链接》。 2. 在弹出窗口中键入 URL。 3. 突出显示要超级链接的文本并单击 《创建链接》（在弹出窗口中）。 4. 保存自选设置。 注释 **:** 如果图像或 URL 位于 HTML 编辑器的左上方，则弹出窗口会与之重叠。由于弹出窗口无法移动，因此必须在编辑器的其它地方创建所需文本，然后将其剪切并粘贴到正确位置。
《添加图像》按钮	**在 Mozilla 中：** 1. 将鼠标焦点放置到要插入图像的位置，然后单击 《添加图像》。 2. 键入 URL 和文本，然后在弹出窗口中单击 《创建图像》。 3. 保存自选设置。 **在 IE 中：** 1. 单击 《添加图像》。 2. 在弹出窗口中键入 URL 和文本，然后将鼠标焦点放置到要插入图像的位置，并在弹出窗口中单击 《创建图像》。 3. 保存自选设置。 注释 **:** 如果图像或 URL 位于 HTML 编辑器的左上方，则弹出窗口会与之重叠。由于弹出窗口无法移动，因此必须在编辑器的其它地方创建所需文本，然后将其剪切并粘贴到正确位置。

功能	提示
《关键字》下拉列表：特性	这些是可用于此实体的特性集。
《关键字》下拉列表：命令	这些命令允许组织结构图入口小程序起动其它身份入口小程序或内置功能，如 IM 或电子邮件工具。 ◆ **IM 操作按钮** - 创建发送 IM 的按钮 ◆ **邮件操作按钮** - 创建发送电子邮件的按钮 ◆ **组织结构图操作按钮** - 创建按钮以切换到另一关系，且以所选实体实例为父实例 ◆ **信息操作按钮** - 起动细节入口小程序 有关生成的按钮的示例，请参见 “内置链接”在第 241 页 。

功能	提示
URL	**OrgChart 导航 URL 链接** - 允许指定要显示为链接的 URL 或实体特性。用户单击此链接时，组织结构图入口小程序会重新显示，且单击的实体会成为根节点。

限制：

此功能仅在关系中的父实体和子实体是相同对象类型时才有效。例如，在经理 - 员工关系中，两者都是用户。

用法提示：

要使用此关键字，请执行以下操作：

1. 单击 《查看来源》。
2. 使用以下语法键入 @NavUrl 关键字：

```
<a href="javascript:$[[@NavUrl]]">someText</a>
```

其中 *someText* 是运行时显示的链接或实体特性。在下面的示例中，《单击此处》将成为可单击的链接。

```
<a href="javascript:$[[@NavUrl]]">Click here</a>
```

在下面的示例中， FirstName 特性将成为可单击的链接：

```
<a href="javascript:$[[@NavUrl]]">$[[FirstName]]</
a>
```

用法限制：

在 Internet Explorer 中，**不能**使用以下语法。

```
<a href="$[[@NavUrl]]">someText</a>
```

保存操作时， Internet Explorer 会添加以下内容：

```
http://context before $[[@NavUrl]]
```

这就意味着

```
<a href="$[[@NavUrl]]">someText</a>
```

会变成

```
<a href="http://localhost/.../
$[[@NavUrl]]">someText</a>
```

并且在运行时这将**不能**正确显示。

功能	提示
	组织结构图导航单击链接 - 对 onClick 事件使用此关键字。（仅可刷新组织结构图入口小程序区域，而不是整个页。） **用法提示：** 要使用此关键字，，请执行以下操作： 1. 单击 《查看来源》。 2. 使用以下语法键入 @NavClick 关键字： `<A href="javascript:return false;" onClick="$[[@NavClick]]">$[[SomeAttribute]]</A>` 其中 *SomeAttribute* 是将成为可单击链接的实体特性。 《javascript:return false;》是必需的。省略它会导致错误。

要保存定义的布局，请单击 《提交》。

使用外部编辑器 可以通过以下方法使用 HTML 外部编辑器：

1 使用自选设置中可用的 HTML 布局编辑器创建实体特性、命令和关键字的 HTML 源文件。

2 将 HTML 源文件复制到所选编辑器中。

3 根据需要进行更改。

4 编辑完成后，将 HTML 源文件复制回 HTML 布局编辑器自选设置。

18.2.3 动态装载图像

要显示储存在 Identity Vault 中的图像 （如用户照片），可以将特性名称添加到名片中。例如，将 User Photo 特性添加到名片布局可显示用户照片。

如果图像储存在 Identity Vault 以外，则需要在 HTML 编辑器中的 《查看来源》方式下使用 IMG: 标签，方法如下所示：

1 转到组织结构图入口小程序的自选设置，并访问 HTML 编辑器。

2 单击 《查看来源》。

3 使用 IMG: 标签按照如下语法将位置、特性键和文件扩展名组合在一起：

```
$[[IMG:”URL” + attribute-key-name + ”fileextension”]]
```

如果已按姓氏将员工照片储存为 JPG 图像，并且放在应用程序服务器的 /images 子目录中，则要使用以下示例中的语法：

```
$[[IMG:"http://myhost:8080/images/"+LastName+".jpg"]]
```

运行时，组织结构图会将 URL 与 LastName 特性和文件扩展名 .jpg 连结在一起。

请注意， HTML 编辑器支持灵活的语法。它支持文本和特性的任意组合，语法如下：

```
$[[IMG:"some text" + attribute-key-name + ...]]
```

口令管理入口小程序参照 19

本章说明如何向 Identity Manager 用户应用程序添加口令自助服务和用户鉴定功能。包括以下主题：

19.1 准备口令管理

要 Identity Manager 用户应用程序可以支持口令自助服务和用户鉴定，需要了解以下内容：

19.1.1 关于口令管理功能

Identity Manager 用户应用程序支持的口令管理功能包括用户鉴定和口令自助服务。使用这些功能时，它们可使应用程序：

- 提示登录信息 （用户名和口令），以便通过 Novell eDirectory 进行验证
- 向用户提供更改口令自助服务
- 向用户提供忘记口令自助服务 （包括根据需要提示询问应答、显示口令提示或允许口令更改）
- 向用户提供询问问题自助服务
- 向用户提供口令提示自助服务

19.1.2 eDirectory 所需的设置

使用大部分口令自助服务和用户鉴定功能之前，需要在 eDirectory 中进行以下设置：

- 启用 《通用口令》
- 创建一个或多个 《口令策略》
- 为用户指派适当的口令策略

口令策略是管理员定义的规则集合，用于指定创建和替换用户口令的准则。Novell Identity Manager 利用 *NMAS* (Novell Modular Authentication Service) 来实施在 eDirectory 中指派给用户的口令策略。

可以使用 *Novell iManager* 来执行所需的设置步骤。例如，以下是某人在 iManager 中定义 DocumentationPassword 策略的示例。



此口令策略指定：

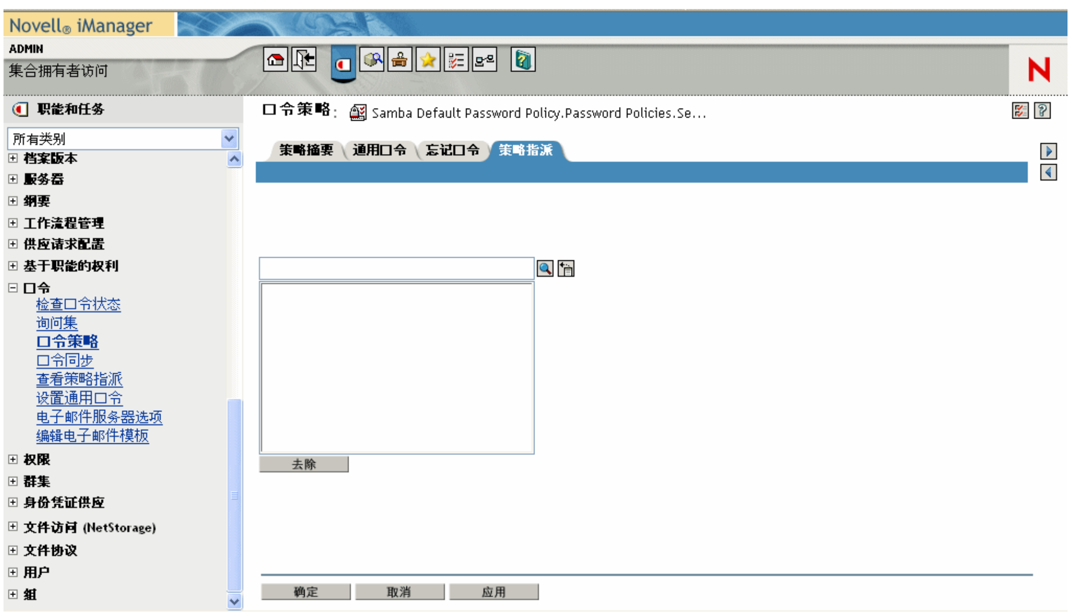
- 《通用口令》设置



◆ 处理 《忘记口令》情况的设置



◆ 将策略应用于特定用户的 《指派》。



有关在 eDirectory 中设置通用口令和口令策略的更多信息，请参见 《Novell Identity Manager 管理指南》(http://www.novell.com/documentation/dirxml20/index.html)。

19.2 关于口令入口小程序

要在 Identity Manager 用户应用程序中实现口令自助服务和用户鉴定功能，需使用以下入口小程序：

入口小程序	说明
“IDM 登录入口小程序”在第 261 页	IDM 登录提供了由 Identity Manager 支持的强大用户鉴定（通过通用口令、口令策略和 NMAS）。IDM 登录入口小程序将根据登录时的需要重定向到其它口令入口小程序。
“IDM 询问应答入口小程序”在第 262 页	此自助服务入口小程序允许用户进行以下操作： ◆ 设置管理员定义的询问问题的有效应答，并设置用户定义的询问问题和应答 ◆ 更改管理员定义的询问问题的有效应答，并更改用户定义的询问问题和应答
“IDM 提示定义入口小程序”在第 263 页	此自助服务入口小程序允许用户设置或更改其口令提示（在忘记口令情况下，会以线索的形式显示或在电子邮件中发送此口令提示）。
“IDM 更改口令入口小程序”在第 264 页	此自助服务入口小程序允许用户根据指派的口令策略更改（重设置）他们的通用口令。它使用此策略显示新口令必须符合的规则。 如果未启用通用口令，则此入口小程序将更改用户的 eDirectory（简单）口令，这在用户口令限制中是允许的。
“IDM 忘记口令入口小程序”在第 266 页	此自助服务入口小程序使用询问 / 应答鉴定是否允许用户得到有关其口令的信息（从 NMAS）。结果取决于所指派的口令策略，可能包括： ◆ 在屏幕中显示用户的口令提示 ◆ 用电子邮件将提示发送给用户 ◆ 用电子邮件将口令发送给用户 ◆ 提示用户重设置（更改）口令

19.2.1 口令自助服务入口小程序方式

口令自助服务入口小程序（IDM 询问应答、IDM 提示定义和 IDM 更改口令）以两种方式进行操作：

方式	说明	运行时行为
独立方式	入口小程序在共享页中独立运行。	◆ 如果入口小程序运行**成功**，则显示成功讯息，其中还提供用于再次执行此操作的链接。 ◆ 如果入口小程序运行**不成功**，则以现有形式显示错误讯息。
委托方式	入口小程序在页中显示为登录时的验证检查结果。	◆ 如果入口小程序运行**成功**，则用户重定向到新的入口小程序或用户应用程序的主页。不显示成功讯息。 ◆ 如果入口小程序运行**不成功**，则以现有形式显示错误讯息。

19.3 IDM 登录入口小程序

IDM 登录入口小程序执行由 Identity Manager 支持的强大用户鉴定 （通过通用口令、口令策略和 NMAS）。IDM 登录入口小程序将根据登录时的需要重定向到其它口令入口小程序。



19.3.1 要求

IDM 登录入口小程序具有以下要求：

主题	要求
口令策略	除非要使用高级口令规则或允许用户单击 《忘记口令》链接，否则此入口小程序不需要口令策略。
通用口令	除非要使用具有高级口令规则的口令策略，否则此入口小程序不需要启用通用口令。
SSL	此入口小程序要使用 SSL，因此请确保已正确配置应用程序服务器，以便支持 SSL 连接到 LDAP 域。

19.3.2 用法

要使用 IDM 登录入口小程序，需要了解以下内容：

- “IDM 登录如何重定向到其它入口小程序”在第 261 页
- “使用宽限登录”在第 262 页

IDM 登录如何重定向到其它入口小程序

运行时， IDM 登录入口小程序将根据完成登录过程需要执行的操作来重定向到其它口令入口小程序。例如：

如果用户	IDM 登录重定向到
单击 《忘记口令》链接	“IDM 忘记口令入口小程序”在第 266 页
需要设置询问问题和应答	“IDM 询问应答入口小程序”在第 262 页

如果用户	IDM 登录重定向到
需要设置口令提示	“IDM 提示定义入口小程序”在第 263 页
需要重设置无效口令	“IDM 更改口令入口小程序”在第 264 页

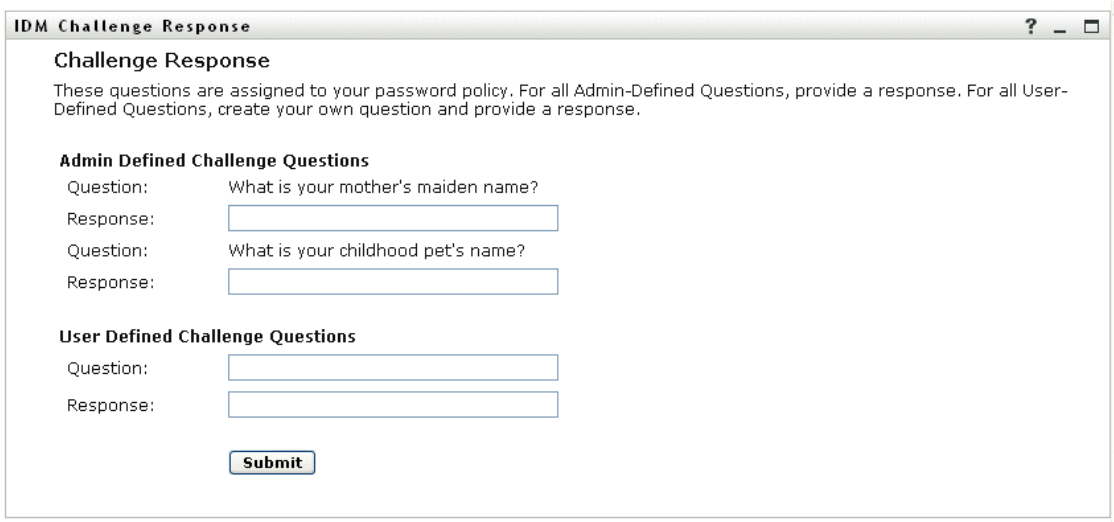
使用宽限登录

如果使用宽限登录，则 IDM 登录入口小程序将显示警告讯息，要求更改口令并指明剩余的宽限登录次数。如果是最后一次登录，则 IDM 登录入口小程序将重定向到 IDM 更改口令入口小程序。

19.4 IDM 询问应答入口小程序

此自助服务入口小程序允许用户进行以下操作：

- 设置管理员定义的询问问题的有效应答，并设置用户定义的询问问题和应答
- 更改管理员定义的询问问题的有效应答，并更改用户定义的询问问题和应答



19.4.1 要求

IDM 询问响应入口小程序具有以下要求：

主题	要求
口令策略	此入口小程序需要已启用忘记口令的口令策略和询问集。
通用口令	此入口小程序不需要启用通用口令。

主题	要求
eDirectory 配置	此入口小程序要求授予用户应用程序管理员对已登录用户所驻留的树枝的主管权限。被授予这些特权的用户可以向机密存储区写入询问应答。 例如，假设 LDAP 域管理员是 cn=admin, ou=sample, n=novell，而您以 cn=user1, ou=testou, o=novell 登录。需要将 cn=admin, ou=sample, n=novell 指派为 **testou** 的受托者，并为 **[All attribute rights]** 授予主管权限。

19.4.2 用法

要使用 IDM 询问应答入口小程序，需要了解以下内容：

- "登录时如何使用 IDM 询问应答"在第 263 页
- "在用户应用程序中如何使用 IDM 询问应答"在第 263 页

登录时如何使用 IDM 询问应答

登录过程中，每当用户需要设置询问问题及应答时，IDM 登录入口小程序 (在第 261 页) 便自动重定向到 IDM 询问应答入口小程序（例如，管理员在 iManager 中将用户指派给口令策略后，用户首次尝试登录到应用程序。口令策略必须启用忘记口令并包括询问集）。

在用户应用程序中如何使用 IDM 询问应答

默认情况下，用户应用程序为用户提供了更改询问问题和应答的自助服务。

19.5 IDM 提示定义入口小程序

此自助服务入口小程序允许用户设置或更改其口令提示（在忘记口令情况下，会以线索的形式显示或在电子邮件中发送此口令提示）。



19.5.1 要求

IDM 提示定义入口小程序具有以下要求：

主题	要求
口令策略	此入口小程序需要已启用忘记口令的口令策略和询问集。
通用口令	此入口小程序不需要启用通用口令。

19.5.2 用法

要使用 IDM 提示定义入口小程序，需要了解以下内容：

- “登录时如何使用 IDM 提示定义”在第 264 页
- “在用户应用程序页中使用 IDM 提示定义”在第 264 页

登录时如何使用 IDM 提示定义

登录过程中，每当用户需要设置他们的口令提示时， IDM 登录入口小程序 (在第 261 页) 便自动重定向到 IDM 提示定义入口小程序 （例如，管理员在 iManager 中将用户指派给口令策略后，用户首次尝试登录到应用程序。口令策略将启用忘记口令并将操作设置为用电子邮件将提示发送给用户或在页面中显示提示）。

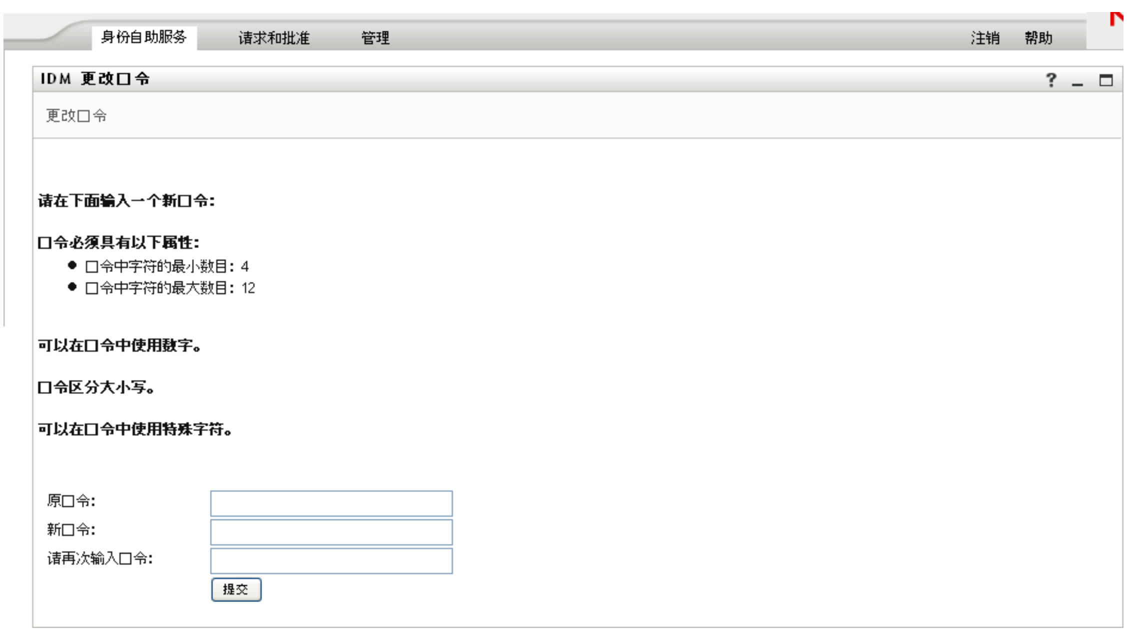
在用户应用程序页中使用 IDM 提示定义

默认情况下，用户应用程序向用户提供了更改其口令提示的自助服务。

19.6 IDM 更改口令入口小程序

此自助服务入口小程序允许用户根据指派的口令策略更改 （重设置）他们的通用口令。它使用此策略显示新口令必须符合的规则。

如果未启用通用口令，则此入口小程序将更改用户的 eDirectory （简单）口令，这在用户口令限制中是允许的。



19.6.1 要求

IDM 更改口令入口小程序具有以下要求：

主题	要求
目录提取层配置	此入口小程序不需要目录提取层配置。
口令策略	除非要使用高级口令规则 （启用通用口令），否则此入口小程序不需要口令策略。
通用口令	要对通用口令使用此入口小程序，则必须在用户指派的口令策略的高级口令规则中启用 《允许用户初始化口令更改》设置。
	要对 eDirectory （简单）口令使用此入口小程序，则必须在用户的口令限制中启用 《允许用户更改口令》设置。

19.6.2 用法

要使用 IDM 更改口令入口小程序，需要了解以下内容：

- "登录时如何使用 IDM 更改口令"在第 265 页
- "在用户应用程序中使用 IDM 更改口令"在第 265 页

登录时如何使用 IDM 更改口令

登录过程中，每当用户需要重设置无效口令 （例如，管理员执行了需要用户重设置他们的口令的口令策略后，用户首次尝试登录到应用程序）时，IDM 登录入口小程序 (在第 261 页) 便自动重定向到 IDM 更改口令入口小程序。

如果用户所指派的口令策略将重设置口令指定为忘记口令时的操作， IDM 忘记口令入口小程序 (在第 266 页) 也会自动重定向到 IDM 更改口令。

在用户应用程序中使用 IDM 更改口令

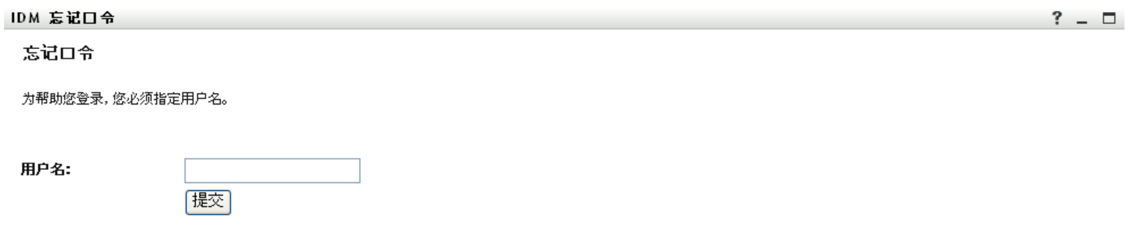
默认情况下，用户应用程序使用 IDM 更改口令入口小程序向用户提供口令更改自助服务。例如：



19.7 IDM 忘记口令入口小程序

此自助服务入口小程序使用询问 / 应答鉴定是否允许用户获得有关他们的口令的信息。结果取决于所指派的口令策略，可能包括：

- 在屏幕中显示用户的口令提示
- 用电子邮件将提示发送给用户
- 用电子邮件将口令发送给用户
- 提示用户重设置 （更改）口令



19.7.1 要求

IDM 忘记口令入口小程序具有以下要求：

主题	要求
口令策略	此入口小程序需要已启用忘记口令的口令策略和询问集。
通用口令	此入口小程序不需要启用通用口令 （除非要支持以下忘记口令操作：重设置口令或用电子邮件将口令发送给用户）。

19.7.2 用法

要使用 IDM 忘记口令入口小程序，需要了解以下内容：

- "如何在登录过程中使用 IDM 忘记口令" 在第 266 页
- "配置用于发送电子邮件操作的环境" 在第 267 页
- "IDM 忘记口令自选设置" 在第 267 页

如何在登录过程中使用 **IDM** 忘记口令

在登录过程中，如果用户单击 《忘记口令》链接，则 IDM 登录入口小程序 (在第 261 页) 将重定向到 IDM 忘记口令入口小程序。显示 IDM 忘记口令时，此入口小程序将执行以下操作：

1. 提示输入用户名。
2. 重定向到 IDM 登录入口小程序 (在第 261 页) 以对该用户执行询问 / 应答鉴定。
3. 执行忘记口令操作，该操作是在已签定的用户指派口令策略中指定。它将执行以下操作之一：
    - 重定向到 IDM 更改口令入口小程序 (在第 264 页)，以便用户可以重设置口令

- 通过电子邮件将口令或提示发送给用户
- 显示提示

注释 **:** IDM 忘记口令入口小程序不能单独使用。这意味着不能将其添加到用户应用程序中的共享页中。将此入口小程序放置到页上会产生潜在的安全隐患，即未经用户确认或许可，有人会在无人照管的计算机上更改口令。

配置用于发送电子邮件操作的环境

如果要支持忘记口令电子邮件发送操作，需要确保正确设置电子邮件通知服务器：

1 在 eDirectory 服务器上使用万维网浏览器访问 *iManager*，并以管理员身份登录。

2 转至 《职能和任务》 > 《口令》并选择 《电子邮件服务器选项》。

3 指定相应的设置，然后单击 《确定》。

IDM 忘记口令入口小程序使用两个电子邮件模板。在 iManager 中，可以在 《职能和任务》 > 《口令》 > 《编辑电子邮件模板》中找到这两个模板。它们的名称为：

- 口令提示请求
- 口令请求

可以根据应用程序的需要更改这些模板的内容 （但是不可以更改结构）。

IDM 忘记口令自选设置

IDM 忘记口令入口小程序提供下列自选设置：

自选设置	细节
login-sequence	要使用的 NMAS 登录顺序。在本版本中，入口小程序仅支持**询问应答**。
ldap-sslport	要使用的安全 LDAP 端口。默认端口为 **636**。
allow-wildcard	键入用户名时用户是否可以键入通配符。默认设置为 **False**。
encoding	要使用的字符编码。默认设置为 **utf-8**。

搜索列表入口小程序参照

20

本章描述如何设置和自定义与 Identity Manager 用户应用程序一起使用的搜索列表入口小程序。包括以下主题：

20.1 关于搜索列表

搜索列表入口小程序允许用户搜索和显示 Identity Vault 的内容。它是 Identity Manager 用户应用程序 《身份自助服务》选项卡中的 《目录搜索》操作的基础。 《目录搜索》操作配置为允许用户搜索用户、组和任务组，但是可以修改此操作以更改可搜索对象和特性的范围。

以下示例说明 《目录搜索》操作如何允许用户定义搜索准则。



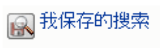
用户界面要素	说明
搜索主题	用户选择要搜索的对象类型。 有关定义此列表内容的更多信息，请参见“设置搜索列表自选设置”在第 275 页 。

用户界面要素	说明
使用该准则	用户通过从下拉列表中选择特性和搜索运算符来定义搜索准则。 用户选择 《高级搜索》时，可以指定搜索条件分组的多行和多块，这些分组可以被设置为包含 (AND) 或排它 (OR)。 有关定义可搜索特性的更多信息，请参见 “设置搜索列表自选设置” 在第 275 页 。
搜索	运行指定的搜索准则。 有关定义默认搜索的更多信息，请参见 “设置搜索列表自选设置” 在第 275 页 。
我保存的搜索 我保存的搜索	允许用户运行、编辑或删除以前保存的搜索。
高级搜索 高级搜索	和 《搜索》按钮一样，它允许用户添加搜索准则的行或块，但在 《高级搜索》中，用户可以指定搜索条件分组的多行和多块，此分组可以被设置为包含 (AND) 或排它 (OR)。 有关定义可搜索特性的更多信息，请参见 “设置搜索列表自选设置” 在第 275 页 。

本示例说明输入 *First name starts with A* （名打头字母 A）的搜索准则后，入口小程序将如何显示 （使用样本数据）：



可以配置搜索列表入口小程序以使用以下任何功能：

用户界面要素	说明
《身份》、《位置》和 《组织》选项卡	用户单击其中一个选项卡即可看到以不同方式显示的结果列表。 有关格式的更多信息，请参见 “关于结果列表显示格式”在第 272 页 。
我保存的搜索 	允许用户选择以前保存的搜索。
保存搜索 	允许用户保存搜索准则并根据需要返回保存的搜索。将搜索保存到当前登录用户的 srvprvQueryList 特性中。
导出结果 	允许用户以不同格式导出搜索结果。
修改搜索 	允许用户更改搜索准则。
新搜索 	允许用户定义新搜索。

默认情况下，搜索列表也允许终端用户：

- 打印搜索结果
- 从结果列表中起动电子邮件
- 从结果列表中起动细节入口小程序

20.1.1 关于结果列表显示格式

可以定义如何将从 Identity Vault 搜索返回的数据显示给终端用户。可以用以下一种或多种页面类型组织数据：

- 身份页 - 通常包含联系信息，如下所示：



- 位置页 - 通常包含位置信息，如下所示：



- 组织结构页面 - 通常包含组织层次结构信息，如下所示：



可以使用入口小程序的复合自选装置定义其它结果列表格式。例如，如果 Identity Vault 纲要包含有关员工技能或认证的信息，则可以设置结果列表以显示此信息。

根据入口小程序的配置，终端用户可以：

- 选择要搜索的 Identity Vault 对象类型 （例如，用户和组）
- 指定要搜索的准则 （例如，名 打头字母、姓 包括等）
- 选择要查看搜索结果的显示格式
- 更改排序顺序

20.2 配置搜索列表入口小程序

若要配置搜索列表入口小程序，请遵循以下一系列步骤：

步骤	任务	说明
1	定义： ◆ 允许用户搜索的实体和特性 ◆ 显示结果列表的方法	可以使用和 Identity Manager 用户应用程序一起安装的预定义目录搜索操作。可以修改此操作或创建自己的目录搜索操作。 有关更多信息，请参见 “设置搜索列表自选设置” 在第 275 页 。
2	验证已在目录提取层中定义了用于搜索的实体和特性集。	有关更多信息，请参见第 4 章 “配置目录提取层” 在第 69 页 。
3	确定用户如何访问入口小程序。	希望用户从现有页还是从新页面起动此入口小程序？ 有关页的更多信息，请参见第 7 章 “页管理” 在第 125 页 。
4	设置入口小程序的自选设置	搜索列表入口小程序的自选设置允许定义： ◆ 每个结果列表格式显示的特性 ◆ 搜索将产生结果列表显示格式 ◆ 结果列表格式的默认排序顺序 有关更多信息，请参见 “设置搜索列表自选设置” 在第 275 页
5	测试设置	验证结果列表是否显示需要的特性。
6	设置 eDirectory 权限并建立增强性能所需的所有索引	eDirectory 权限： 执行搜索 ◆ 执行搜索的用户需要具有所有被搜索用户或对象的**浏览**权限。 保存搜索 （对于非管理员用户）： ◆ 执行搜索的组织单元和组织的**受托者**。 ◆ 用户需要写权限、自身权限和主管权限。 **性能增强 -** 可以通过将 eDirectory 值索引添加到特性 （搜索基于此特性）来提高搜索性能。

有关定义不同结果列表显示格式的更多信息，请参见 “设置搜索列表自选设置”在第 275 页 。

20.2.1 目录提取层设置

必须在目录提取层定义可以从搜索准则下拉列表中选择的实体和特性以及从 Identity Vault 搜索中返回的数据。下表显示可以为搜索列表使用的实体和特性设置的属性。

定义类型	设置	目录提取层值
实体	查看	选中 (True)
特性	启用	选中 (True)
	搜索	选中 (True) 为 False 时，不能定义基于此特性的搜索或将其包含在结果列表格式中
	隐藏	取消选择 (False) 由于在搜索过程中搜索列表入口小程序不检查隐藏属性值（因为其妨碍性能），因此搜索被设置为选中 (True) 的所有特性还必须将 《隐藏》设置为取消选择 (False)。 假定 User1 将 HomePhone 特性设置为 hide=true （在 eDirectory 中）。由于 HomePhone 为可搜索的，因此搜索列表将检索记录，但不检查其它特性值 （因为这会影响性能）。如果其它用户搜索到 HomePhone 特性的精确匹配，则此隐藏记录将在结果列表中显示。

其它目录提取层设置 目录提取层的数据类型、格式类型、过滤器和搜索范围也将影响搜索列表入口小程序。数据类型和格式类型影响其外观，而过滤器和搜索范围则影响返回数据的数量。

有关更多信息，请参见 “使用实体和特性”在第 79 页 。

20.2.2 设置搜索列表自选设置

可以定义两种类型的自选设置：

- “搜索自选设置”在第 276 页
- “结果列表格式自选设置”在第 278 页

搜索自选设置

搜索自选设置包含在单个自选设置页中：



搜索自选设置定义如下：

自选设置	操作

默认方式	指定在用户首次访问入口小程序时，该入口小程序将如何显示。值为：
	
	基本搜索 - 允许用户输入单个搜索准则。例如：
	
	`First Name starts with A`
	
	高级搜索 - 允许用户在一个或多个搜索块中定义多个搜索准则。用户可以在搜索准则或搜索块中使用 and/or 逻辑运算符。例如，用户可以创建如下搜索：
	
	`(First Name starts with A or First Name starts with B) and (Region = Northeast or Region = Southeast)`
	
	或者
	
	`(First Name starts with A and Last Name starts with B) or (First Name starts with B and Last Name starts with A)`
	
	我保存的搜索 - 显示当前登录用户保存的搜索列表。这些搜索保存在用户的 srvprvQueryList 特性中。
	
	注释：用户可以在运行时通过执行或编辑搜索或单击入口小程序底部按钮，访问上述任何一种方式。

分页	一次显示的最大行数。
结果限制	搜索返回的最大匹配数。如果设置为 0，则最大值将遵从目录提取层的设置。
搜索和列表的复杂自选设置	单击以简化： ◆ 要搜索的实体 ◆ 结果集类型 ◆ 包含在该页中的特性以及特性在页中显示的顺序 默认情况下，搜索中包括目录提取层中列出的特性为 view=true 的所有对象。实体的特性列表派生于目录提取层中列出的并定义为 enable=true 的特性。

结果列表格式自选设置

复合自选设置页允许定义要包含在搜索中的实体以及格式化结果列表格式的方法。默认的自选设置页如下所示：



复合自选设置包含：

自选设置	操作
实体定义	用于搜索的每个有效实体 (view=true) 在此自选设置页上都有一个相应的实体定义块。这些自选设置用于： ◆ 定义包含在搜索中的对象。 ◆ 修改结果列表格式定义 （例如，添加和去除显示的特性以及默认的排序顺序）。 ◆ 单击 《实体定义》行中的 《删除》按钮，可以去除不希望搜索的对象。这样就删除了整个的实体定义块。 可以通过单击 《添加实体定义》（位于页面底部）并完成填写向导选择面板，将对象稍后添加回搜索中。 **提示：**如果对象不出现在此列表而出现在目录提取层列表中，请检查**视图**修改器 （位于实体对象上）。如果该实体被设置为 False，则身份入口小程序将无法使用该实体。
将电子邮件显示为图标	如果为 True 且在结果列表中指定了 Email 特性时，则电子邮件将显示为图标。如果为 False，则 Email 特性显示完整的电子邮件地址。电子邮件特性 （无论为文本或图标）为可单击的 mailto: 链接。
结果列表类型 （默认）	指定当前实体的结果列表默认格式。只有当前用户未选择其它格式时，才使用默认格式。
结果列表显示格式块	指定显示格式 （例如身份、位置或组织结构页面）并包含包含在类型中的特性集。 **要去除结果列表类型，请执行以下操作：** ◆ 单击结果列表类型旁边的 《删除》按钮。 此操作将删除页面类型和搜索中与其相关联的所有特性。 **要添加结果集页面，请执行以下操作：** ◆ 单击 《展开》按钮，并从选择列表中选择结果集格式。

自选设置	操作
特性	指定为特定显示格式显示的特性集。 **要添加或去除特性，请执行以下操作：** ◆ 单击 《修改特性》按钮。 ◆ 要添加特性，请从可用特性列表中选择。 ◆ 单击箭头，将其移动到 《选定》列表中。执行相反的操作则可以从结果列表中去除特性。 ◆ 要对特性列表重新排序，请单击 《选定》列表右侧的向上箭头和向下箭头。 ◆ 单击 《提交》。 **特性和数据类型** - 特性的数据类型影响其显示方式。例如，如果将特性定义为本地列表或全局列表的子类型，则将在基本搜索准则或高级搜索准则屏幕的下拉列表框中显示可能的值。如果类型为 DN，则显示 《查找器》按钮和 《历史》按钮，允许用户在基本搜索准则或高级搜索准则屏幕中选择值，而 DN 则在结果列表中被解析为用户友好的显示方式。数据类型和子类型也限制向用户显示的比较运算符，以确保仅构造有效比较。 有关更多信息，请参见第 4 章 "配置目录提取层"在第 69 页 。
结果列表显示格式块排序	结果列表排序顺序基于此特性。仅当结果集类型不是当前用户会话的显示格式时，默认排序顺序才生效。 **多值特性和单值特性** - 结果列表中显示的记录数将随排序特性为单值还是多值而变化。虽然总匹配数相同，但单值特性排序通常会产生多个记录。这是因为多值特性的每个值都会单独在一行显示。

完成自选设置面板

要验证已提交的有效项，请单击 《提交》。如果某项无效，自选设置页的顶部会显示一条错误讯息。在解决所有错误后，请单击 《返回到列表视图》，然后单击 《保存自选设置》。

设计和管理供应请求

V

以下章节介绍如何使用 Identity Manager 的预置模块功能。

基于工作流程的配置信息提供的介绍 21

本章提供基于工作流程的配置信息提供的概述。包括以下主题：

21.1 关于基于工作流程的配置信息提供

Identity Manager 的一个主要功能是基于工作流程的配置信息提供，这是管理用户访问组织中安全资源的进程。这些资源可以包含诸如用户帐户、计算机和数据库之类的数字实体。在此版本中，受供资源被映射到 Identity Manager 权利。

Identity Manager 可以为大量的供应请求提供服务。供应请求是用户或系统用于授予或取消访问组织资源的操作。这些请求可以由终端用户通过 Identity Manager 用户应用程序直接初始化，也可以通过在 Identity Vault (eDirectory) 中响应发生的事件间接初始化。

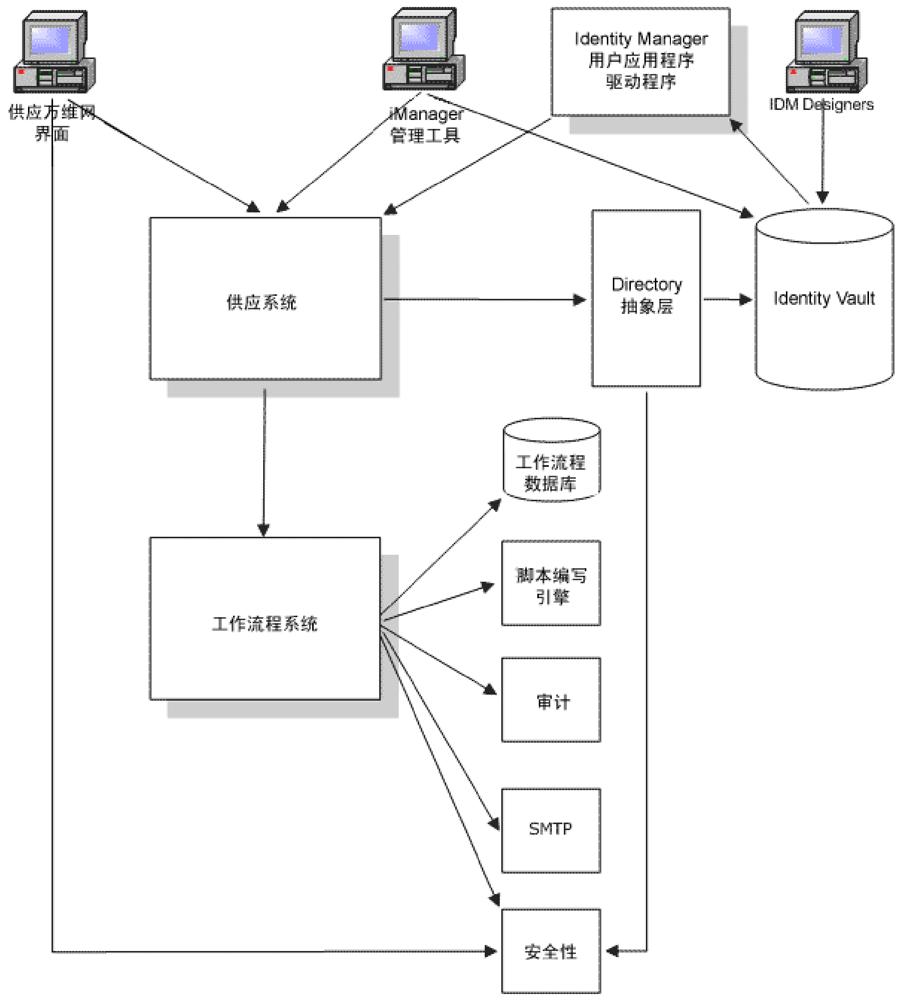
供应请求需要从组织中的一个或多个人中获得许可权限时，此请求将启动工作流程。工作流程协调完成请求所需的批准。某些供应请求需要获得个人批准；而另外一些请求则需要获得多人批准。在某些实例中，可以不经任何批准完成请求。

某些工作流程需要以顺序方式处理，其中每个批准步骤都按顺序执行。而其它一些工作流程则支持并行处理。定义供应请求时，请指定工作流程是支持顺序处理还是并行处理。

Identity Manager 提供一套基于万维网的工具，管理员可以使用此套工具将供应功能构建到用户应用程序中。使用这些工具可以配置供应请求，也可以管理正在进行的工作流程。若要配置供应请求，管理员需要创建将资源联结到工作流程的供应请求定义。

21.1.1 高级体系结构

下图显示 Identity Manager 中包含的基于工作流程供应系统的高级体系结构：



以下部分描述此体系结构的所有部件。

供应万维网接口

Identity Manager 用户应用程序提供万维网接口，终端用户通过此接口提交供应请求并在提交后管理这些请求。用户应用程序还允许应用程序管理员或组织经理指派受托人或代理来供应工作流程。

提示：供应和工作流程操作在 Identity Manager 用户应用程序的 《请求和批准》选项卡中可用。

有关受托人和代理的更多信息，请参见 “供应安全性”在第 291 页 。有关使用用户应用程序的完整详细信息，请参见 《*Identity Manager* 用户应用程序：用户指南》。

iManager 管理工具

iManager 提供可以用来配置和管理供应请求以及与这些请求相关联的工作流程的插件。

若要配置供应请求，则将其联结到受供资源，指定关联的工作流程运行时特征并使此请求可用。初始化供应请求后，则可以使用 iManager 查看工作流程进程状态，重指派工作流程内的活动或在工作流程停止时将其终止。

Identity Manager 用户应用程序驱动程序

除了支持终端用户供应资源的请求， Identity Manager 还允许在响应 eDirectory 中发生的事件时初始化供应请求。Identity Manager 用户应用程序驱动程序监听事件并通过初始化相应的供应请求来进行响应。这些请求可以又依次初始化工作流程以处理批准进程。例如，如果进行了这样的配置， Identity Manager 将执行的方案是：向 eDirectory 中添加新用户时，将自动启动预先指定的供应请求和工作流程。

供应系统

供应系统执行所需的所有处理以初始化并完成供应请求。如果请求需要一项或多项批准，则供应系统依次调用工作流程系统以启动工作流程进程。给予必需的批准后，供应系统按照请求供应资源。

供应系统维护 Identity Vault (eDirectory) 中可用的和未解决的有关供应请求信息。

若要初始化某个请求或执行所需的处理以完成请求，系统将通过目录提取层访问 Identity Vault。

有关目录提取层的详情，请参见第 4 章 “配置目录提取层”在第 69 页 。

工作流程系统

供应请求需要一项或多项批准时，工作流程系统将协调此批准过程。处理过程中，此流程和这些部件进行交互：

- 工作流程数据库
- 底稿编写引擎
- Audit
- SMTP
- 安全系统

工作流程数据库

要跟踪正在执行的工作流程状态，工作流程系统需将信息储存在数据库中。此数据库维护有关工作流程进程实例、工作列表 （队列）和工作流程地址的信息。此外，它还储存在执行工作流程进程中添加的任何注释。

底稿编写引擎

只要工作流程包含必须被求值的动态表达式，工作流程系统都将调用底稿编写引擎。动态表达式可以包含目录提取层中实体的变量、函数、运算符以及参照。

Novell Audit

工作流程系统与 Novell Audit 进行交互以记录有关工作流程进程状态的信息。在处理过程中，工作流程可能会记录已发生的各种事件的信息。然后，用户可以使用 Novell Audit 报告工具查看日志记录数据。

有关设置日志记录的详情，请参见第 5 章 “设置日志记录”在第 109 页。有关控制希望 Identity Manager 用户应用程序生成的日志记录讯息级别的详情，请参见第 12 章 “日志记录配置”在第 193 页。

SMTP

工作流程进程通常会在执行过程中的多个时刻发送电子邮件通知。例如，将一个工作流程活动指派给一个新收件人时，可能会发送电子邮件。

管理员可以在 iManager 中编辑电子邮件模板，并在工作流程进程中使用此模板。在运行时，工作流程系统从 eDirectory 中检索此模板并用适合通知的动态文本替换标记。

通过简单邮件传送协议 (SMTP) 处理电子邮件通知。

有关电子邮件通知所需的基本设置步骤，请参见“配置电子邮件服务器”在第 326 页和“使用安装的电子邮件模板”在第 327 页。有关配置用于工作流程的电子邮件通知的详情，请参见“配置工作流程活动”在第 307 页。

安全性

安全系统处理基于工作流程供应应用程序的各个方面的安全。

有关工作流程安全性的更多信息，请参见“供应安全性”在第 291 页。

21.1.2 供应和工作流程示例

假定用户需要一个 IT 系统中的帐户。若要设置此帐户，用户需要通过 Identity Manager 用户应用程序初始化请求。此请求将启动协调批准过程的工作流程。给予必需的批准后，请求也已完成。此过程有三个基本步骤，概括如下。

第 **1** 步：初始化请求

在 Identity Manager 用户应用程序中，用户通过类别浏览资源列表并选择要供应的一个资源。在 Identity Vault 中，将选择的受供资源与供应请求定义 相关联。供应请求定义是供应系统中最重要的对象。它将受供资源联结到工作流程，工作流程进程通过它开放给终端用户。供应请求定义向用户提供显示初始请求表所需的所有信息，并在初始请求完成后启动工作流程。

在本示例中，用户选择新帐户资源。用户初始化请求时，万维网应用程序从供应系统中检索初始请求表和相关联的初始请求数据说明，该供应系统从供应请求定义获得这些对象。

初始化供应请求时，供应系统将跟踪发起人和收件人。发起人是提出请求的人员。而收件人是接受请求的人员。在某些情况下，发起人和收件人可能是同一个人。

每个供应请求都有与之相关联的操作。此操作指定用户是否要授予或取消资源。

第 **2** 步：批准请求

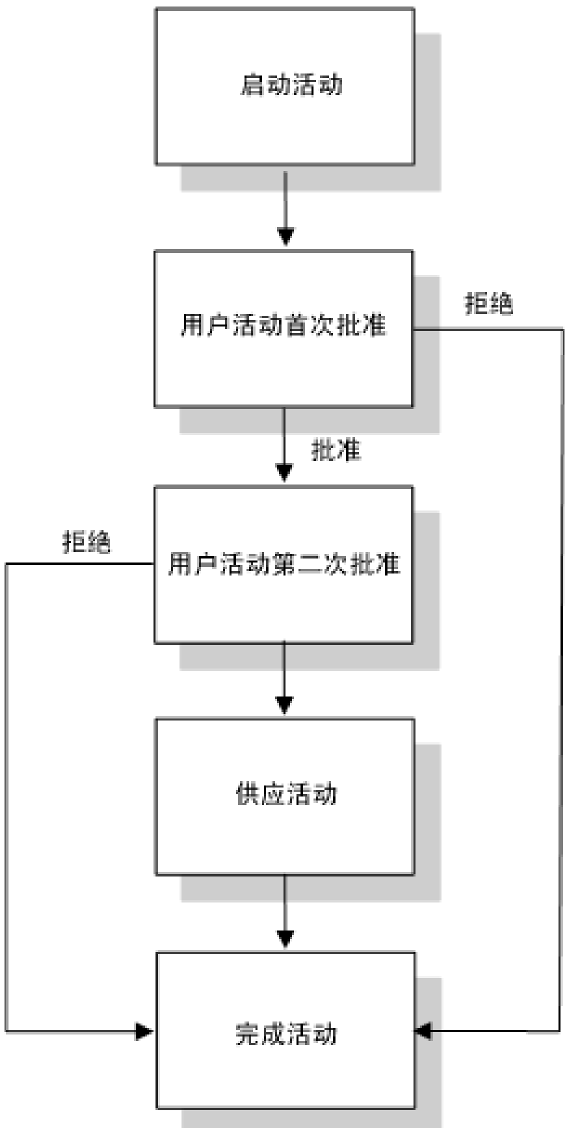
用户初始化请求后，供应系统将启动工作流程进程。工作流程进程协调批准。在本示例中，需要经过两级批准，一级来自用户管理器，另一级来自管理器主管。如果在工作流程中任何用户拒绝批准，则该工作流程终止并拒绝请求。

注释 **:** Identity Manager 附带了一组供应请求模板，这些模板支持高达五级的工作流程批准。在 Identity Manager 的后续版本中，基于 Eclipse 的设计环境将提供允许创建个人自定义工作

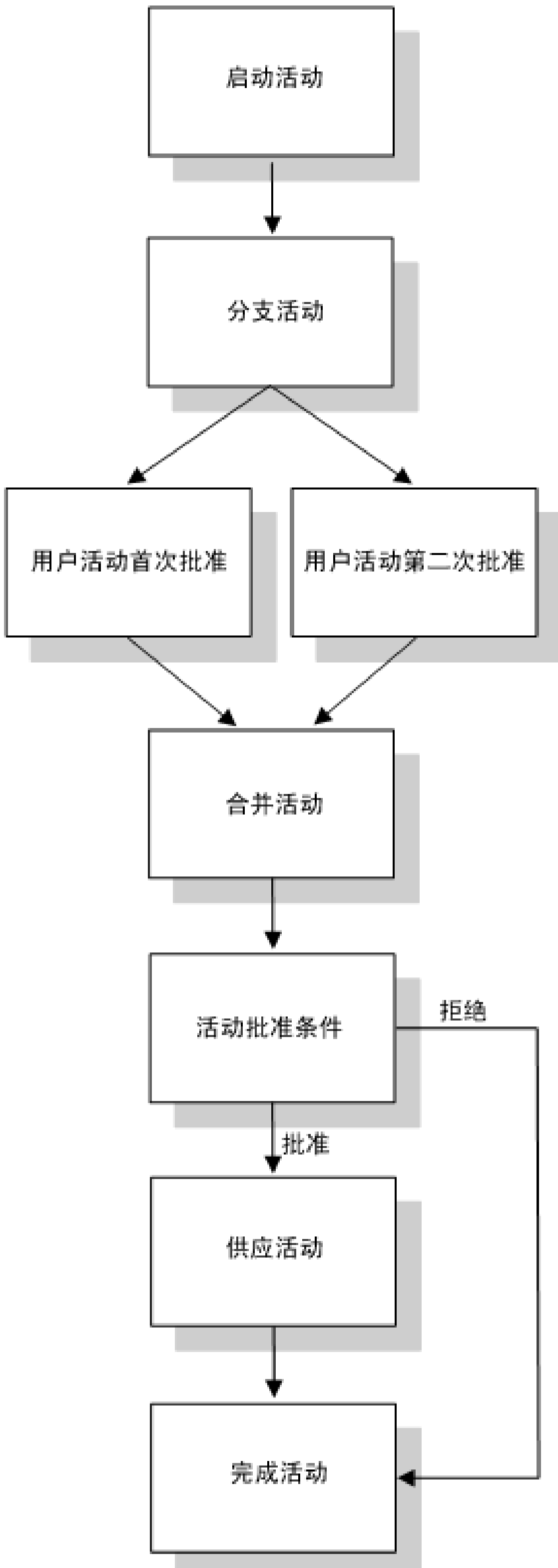
流程进程的工具。有关本版本附带模板的更多信息，请参见“使用已安装的模板”在第 295 页 。

工作流程可以用顺序或并行的方式处理批准。在顺序工作流程中，每个批准任务都必须在下个批准任务开始之前得到处理。在并行工作流程中，用户可以同时处理多个批准任务。

顺序工作流程 以下是包含两个批准级别的顺序工作流程基本设计模式：



并行流程 以下是包含两个批准级别的并行流程基本设计模式：


启动活动
分支活动
用户活动首次批准
用户活动第二次批准
合并活动
活动批准条件
拒绝
批准
供应活动
完成活动

注释：可以轻松更改显示标签 （第一步批准、第二步批准等）以适合应用程序的需求。对于并行流程，可能希望指定不按顺序处理的标签。例如，可能想要指派三个并行批准中的一个批准，三个并行批准中的两个批准等标签。

工作流程定义由下列部件构成

处理部件	说明
活动	活动是表示任务的对象。活动可以向用户显示信息并响应用户的交互，或执行用户不可见的后台功能。 在上述工作流程示例中，以框表示活动。 在 Identity Manager 用户应用程序中，处理批准过程的用户活动被称为**任务**。终端用户可以通过单击 《我的工作》组操作中的 《我的任务》在队列中看到其任务列表。若要查看已处理的特定任务的工作流程活动，用户可以选择此任务并在任务细节表中单击 《查看注释历史》按钮。 若要查看已处理的特定供应请求的工作流程活动，用户可以单击 《我的请求》，选择此请求，然后在请求细节表中单击 《查看注释和流程历史》按钮。 有关 《我的任务》和 《我的请求》操作的更多信息，请参见 *《Identity Manager 用户应用程序：用户指南》*。
链接	链接将工作流程中的活动结合在一起。链接表示要遵循的两个活动间的路径。 活动可以存在多个进来的链接和多个出去的链接。活动有多个出去的链接时，选择的链接取决于活动的**结果**。结果为活动执行的处理的最后结果。例如，用户活动可能有批准的结果或拒绝的结果，这取决于用户采取的**行动**。 在上述工作流程示例中，以箭头表示链接。

开始活动 工作流程进程首先执行开始活动。此活动使用初始请求数据初始化工作文档。它也联结诸如发起人和收件人等多个系统值，以便在底稿表达式中可以使用这些值。

用户活动 执行完开始活动后，工作流程系统将处理转发到该流程中的第一个用户活动中。用户活动为支持用户交互的活动。若要处理这些交互，活动将显示一个表格，该表格给予用户作用于请求的能力。在上述工作流程示例中，第一步批准和第二步批准是用户活动的示例。可以将用户活动标签本地化以满足国际要求。

用户活动可以支持下列一个或多个操作：

- 声明
- 批准
- 拒绝
- 拒收
- 重指派 （仅适用于组织经理和用户应用程序管理员）

注释：表格中的字段和按钮将随请求的资源和配置的工作流程而变化。例如，产品附带的很多模板不支持拒收操作。

用户活动有五个可能的结果：

- 已批准
- 拒绝
- 拒收
- 错误
- 超时

注释：即使用户不进行任何操作，也可能会出现错误结果和超时结果。

如果用户批准请求，工作流程会将控制转发到流程中的下一个活动。如果不再需要批准，就会供应资源。如果用户拒绝了请求，工作项目将被转发到工作流程中的下一个活动并且该请求被拒绝。此外，用户也可以重指派任务 （如果他 / 她是组织经理或用户应用程序管理员），这样可将工作项目置于其它用户的队列中。

注释：产品附带的供应请求模板配置为在请求被拒绝时终止工作流程进程。请求被拒绝时，工作项目会被转发到完成活动中，这会终止流程。

用户活动指派到的用户称为收件人。可通过电子邮件向活动的收件人通知指派的任务。要进行与该活动关联的工作，该收件人可单击电子邮件中的 URL，在工作列表 （队列）中找到任务，然后声明该任务。

收件人必须在指定的时间内响应用户活动，否则活动将超时。通常情况下，超时间隔以小时或天为单位，以使用户有足够的时间进行响应。

活动超时后，工作流程进程可能会试图再次完成该活动，这取决于为该活动指定的重试计数。在某些情况下，工作流程进程可能配置为将已超时的活动上报给另一用户。在这种情况下，会将活动重指派给新的收件人 （例如，该用户的经理），使该用户还有机会完成该活动的工作。如果最后一次重试超时，则可能会将该活动标记为已批准或已拒绝，这取决于工作流程的配置。

条件活动 在执行过程中，工作流程进程可能会执行测试并检查结果，以确定下一步该做什么。条件活动提供此功能。条件活动使用底稿表达式定义要求值的条件。在上面所示的工作流程示例中，批准条件就是条件活动的一个例子。

条件活动支持三种可能的结果：

- True
- False
- 错误

分支和合并活动 在支持并行处理的工作流程中，分支活动允许两个用户在工作项目的不同区域并行操作。用户完成工作后，合并活动会同步流程中进来的分支。

供应活动 供应活动完成供应请求。仅在给出所有必要的批准后，才执行此活动。

有关供应步骤的详情，请参见 “第 3 步：完成请求”在第 291 页 。

完成活动 完成活动是工作流程中的最后一项活动。当完成了工作流程中的所有活动并且流程的最终结果可用时，可以执行完成活动。工作流程系统可通过检查指向完成活动的链接，确定进程的最终状态。当批准链接指向完成活动时，则总流程状态为已批准。如果有任何其它结果 （拒绝、超时或错误）指向完成活动，则总流程状态为被拒绝。

当工作流程过程到达完成活动并且状态为已批准时，批准过程即为完成，也可以完成供应请求。

第 **3** 步：完成请求

供应请求被批准后，工作流程系统就可以开始执行供应步骤。此时，控制被传递回供应系统。

为完成供应请求，供应系统可能会执行 Identity Manager 权利，或直接处理 eDirectory 对象及其特性。在执行供应步骤过程中，它将按照供应数据定义中的说明创建任何相关的对象，并记录对收件人执行供应操作的结果。这可能会涉及设置或去除收件人的特性值，也可能涉及在收件人的多值特性中添加项目或去除项目，具体取决于用户请求的操作是授予还是撤消。涉及的特性为 eDirectory 特性 （可能通过向收件人添加辅助类才可用）。特性值本身可能属于简单类型，也可能属于允许供应系统指定内部子特性值的复杂类型。

21.2 供应配置和管理

要配置供应请求定义，请使用 iManager 将它联结到受供资源，指定关联工作流程的运行时特征，并将它启用以备使用。Identity Manager 附带了一组预部署的供应请求定义和工作流程。可用它们作为模板自行构建供应系统。安装的模板易于使用并且很灵活，足以满足广泛的商业环境要求。要建立系统，请根据已安装的模板定义新的对象，并自定义这些对象以适合组织的需要。

供应请求定义配置完成后，可以使用 iManager 查看正在运行的工作流程进程的状态、重指派工作流程内的活动或在工作流程受阻时将其终止。

有关使用 iManager 进行供应配置和管理的更多信息，请参见第 22 章 “配置供应请求定义” 在第 295 页 和第 23 章 “管理供应工作流程” 在第 317 页 。

21.3 供应安全性

用户登录到 Identity Manager 用户应用程序时，安全系统会鉴定该用户并设置访问控制，以防止非法使用供应和工作流程对象。这样可确保用户只看到那些他或她有权限访问的供应请求定义。除了执行用户应用程序的鉴定和授权服务，安全系统还管理代理和委托指派。

- 受托人是被授权为另一用户执行工作的用户。委托指派适用于特殊的供应请求定义。
- 代理是被授权为一个或多个用户、组或树枝执行任意和所有工作的用户。与委托指派不同的是，代理指派独立于供应请求定义，因此适用于所有的工作和设置。

如果启用了日志记录，则代理或受托人执行的任何操作都将和其他用户执行的操作一起记录。当代理或受托人执行操作时，日志讯息会明确指示，该操作是由代理或受托人代替另一用户执行的。另外，每次定义一个新的代理或委托指派时，都会记录此事件。

如果供应请求定义配置为生成电子邮件通知，将通过电子邮件通知代理和收件人。但不会通过电子邮件通知受托人。

工作流程安全职能 安全系统识别以下安全职能：

职能	说明	权限
用户应用程序管理员	具有全部管理权限的 Locksmith 用户。	允许用户应用程序管理员在 **iManager** 中执行这些任务： ◆ 配置供应请求 ◆ 管理正在进行的工作流程 允许用户应用程序管理员在**用户应用程序**中执行这些任务： ◆ 查看和编辑所有工作流程队列中的所有任务。 ◆ 为系统中的任意用户定义代理和委托指派。 ◆ 查看系统中任意用户的隐藏信息 （隐藏特性）。 ◆ 创建任务组管理员并将他们指派到组。用户应用程序管理员是唯一能创建和指派任务组管理员的用户。 注释 **:** Identity Manager 用户应用程序的 《管理》选项卡提供指派权限的工具，以管理用户应用程序。要使用此选项卡，必须首先以安装时被指定为用户应用程序管理员的用户身份登录。 有关使用用户应用程序安全性功能的详情，请参见第 11 章 “安全性配置” 在第 189 页 。
组织经理	员工直接报告的主管。每个用户仅有一个组织经理。 提示 **:** 组织经理也可看作是管理经理。	允许组织经理进行如下操作： ◆ 查看他 / 她小组的工作流程队列中的所有任务。该功能应用于管理层次结构中的单个级别；因此，组织经理的主管看不到组织经理直接报告的任务。 ◆ 编辑直接报告的任务，除非直接报告中的某项任务所指派到的组的任务组管理员不是组织经理。在此情况下，组织经理可以查看此任务，但不能执行任何编辑操作。上报时，此任务将移动到任务组管理员处，而不是组织经理处。 ◆ 声明任务和取消声明任务，以及向他 / 她小组的成员重指派任务。 ◆ 为他/她本人及其小组的成员定义代理和委托关系。 ◆ 查看他 / 她小组成员的隐藏特性。

职能	说明	权限
任务组管理员	被授权负责与任务组关联的一组任务的用户。任务组是 LDAP 组对象的扩展。每个任务组只能有一个任务组管理员。 任务组管理员由用户应用程序管理员指派。 为组指派任务时，该组的 srvrprvTaskManager 特性包含被指派为任务组管理员的用户的 DN。为提高性能，用户对象上也由一个特性标识出任务组管理员。被指定为任务组管理员的用户的 srvprvIsTaskManager 特性被设置为 True。	允许任务组管理员进行以下操作： ◆ 对于他 / 她被指派为领导的组，可查看和编辑指派给该组的所有任务。 不允许任务组管理员进行以下操作： ◆ 创建资源或收回请求。 ◆ 定义代理或委托关系。 ◆ 查看他 / 她小组成员的隐藏特性。

注释：任何用户都可以查看与他 / 她自身身份关联的隐藏特性。

定义代理和委托关系 要为用户定义代理指派，可使用 Identity Manager 用户界面的《请求和批准》选项卡上的《小组代理指派》页。要为用户定义委托指派，可使用《小组委托指派》页，在《请求和批准》选项卡上也可访问该页。

创建任务组管理员 要为任务组定义任务组管理员，可使用 Identity Manager 用户界面的《身份自助服务》选项卡上的《创建用户或组》页。

有关定义任务组管理员、代理和受托人的完整详细信息，请参见《*Identity Manager* 用户应用程序：用户指南》。

配置供应请求定义 22

本章提供配置供应请求定义的说明。包括以下主题：

22.1 关于供应请求配置插件

要配置供应请求定义，需要使用 iManager 的供应请求配置插件。使用该插件可将供应请求定义联结到受供资源、指定关联工作流程的运行时特征，并启用它以供使用。在此版本中，将受供资源映射到 Identity Manager 权利。

注释 : 还可以运行直接映射到 Identity Vault 特性中的供应请求定义。但是，由于已安装的模板是基于权利的，因此它们不支持这种类型的资源。

可以在 iManager 的 *Identity Manager* 类别中找到供应请求配置插件。此插件的供应请求配置职能中包含供应请求任务。供应请求任务由下列面板组成：

面板	说明
供应驱动程序选择	提供选择 Identity Manager 用户应用程序驱动程序的机会。驱动程序包含一组预部署的供应请求定义，因此需要首先选择驱动程序，然后才能开始配置供应请求。
供应请求配置	可使用提供的工具执行以下操作： ◆ 浏览可用的供应请求定义，并选择一个进行配置 ◆ 基于现有定义创建一个新的供应请求定义 ◆ 设置供应请求定义的属性 ◆ 将供应请求定义指派给受供资源 ◆ 编辑关联工作流程中每项活动的收件人和超时设置 如果要新建供应请求或编辑现有供应请求，此插件会运行《供应请求配置向导》。

22.2 使用已安装的模板

Identity Manager 附带了一组预部署的供应请求定义和工作流程。可用它们作为模板自行构建供应系统。要建立系统，可以根据已安装的模板定义新对象，并自定义这些对象以适应组织需要。

可使用已安装的模板确定完成请求所需的批准步骤数。可以将供应请求配置为：

- 不需要批准
- 需要一步批准
- 需要两步批准

- 需要三步批准
- 需要四步批准
- 需要五步批准

还可以指定希望支持按顺序处理还是并行处理，以及在处理过程中工作流程超时的情况下是批准还是拒绝请求。

有关工作流程设计模式的更多信息，请参见 "供应和工作流程示例"在第 286 页 。

Identity Manager 附带了以下模板：

模板	说明
自我提供批准	允许不经过任何批准即完成供应请求。
一步批准 （批准超时）	完成供应请求需要一步批准。如果活动超时，该活动会批准请求，并且工作项目会转发到下一个活动。
两步顺序批准 （批准超时）	完成供应请求需要两步批准。如果活动超时，该活动会批准请求，并且工作项目会转发到下一个活动。 该模板支持按顺序处理。
三步顺序批准 （批准超时）	完成供应请求需要三步批准。如果活动超时，该活动会批准请求，并且工作项目会转发到下一个活动。 该模板支持按顺序处理。
四步顺序批准 （批准超时）	完成供应请求需要四步批准。如果活动超时，该活动会批准请求，并且工作项目会转发到下一个活动。 该模板支持按顺序处理。
五步顺序批准 （批准超时）	完成供应请求需要五步批准。如果活动超时，该活动会批准请求，并且工作项目会转发到下一个活动。 该模板支持按顺序处理。
一步批准 （拒绝超时）	完成供应请求需要一步批准。如果活动超时，工作流程会拒绝请求。 该模板支持按顺序处理。
两步顺序批准 （拒绝超时）	完成供应请求需要两步批准。如果活动超时，工作流程会拒绝请求。 该模板支持按顺序处理。
三步顺序批准 （拒绝超时）	完成供应请求需要三步批准。如果活动超时，工作流程会拒绝请求。 该模板支持按顺序处理。
四步顺序批准 （拒绝超时）	完成供应请求需要四步批准。如果活动超时，工作流程会拒绝请求。 该模板支持按顺序处理。
五步顺序批准 （拒绝超时）	完成供应请求需要五步批准。如果活动超时，工作流程会拒绝请求。 该模板支持按顺序处理。

模板	说明
两步并行批准（批准超时）	完成供应请求需要两步批准。如果活动超时，该活动会批准请求，并且工作项目会转发到下一个活动。 该模板支持并行处理。
三步并行批准（批准超时）	完成供应请求需要三步批准。如果活动超时，该活动会批准请求，并且工作项目会转发到下一个活动。 该模板支持并行处理。
四步并行批准（批准超时）	完成供应请求需要四步批准。如果活动超时，该活动会批准请求，并且工作项目会转发到下一个活动。 该模板支持并行处理。
五步并行批准（批准超时）	完成供应请求需要五步批准。如果活动超时，该活动会批准请求，并且工作项目会转发到下一个活动。 该模板支持并行处理。
两步并行批准（拒绝超时）	完成供应请求需要两步批准。如果活动超时，工作流程会拒绝请求。 该模板支持并行处理。
三步并行批准（拒绝超时）	完成供应请求需要三步批准。如果活动超时，工作流程会拒绝请求。 该模板支持并行处理。
四步并行批准（拒绝超时）	完成供应请求需要四步批准。如果活动超时，工作流程会拒绝请求。 该模板支持并行处理。
五步并行批准（拒绝超时）	完成供应请求需要五步批准。如果活动超时，工作流程会拒绝请求。 该模板支持并行处理。

工作流程和受供资源 每个供应请求定义中都有一个与工作流程和受供资源联结的预配置联结。可以更改与请求定义关联的受供资源，但不能更改工作流程或其拓扑。

供应请求的类别 每个供应请求模板都联结到一个类别。类别为终端用户组织供应请求提供了一种简便的方法。所有供应请求模板的默认类别是 *Entitlements* （权利）。类别键，即 srvprvCategoryKey 特性的值，为 *entitlements* （小写）。

可以使用目录提取层编辑器自己创建类别。创建新类别时，请确保类别键（srvprvCategoryKey 的值）为小写。这是确保类别在 Identity Manager 用户应用程序中正常工作所必需的。

有关创建供应类别的详情，请参见“使用列表”在第 94 页。

22.3 配置供应请求定义

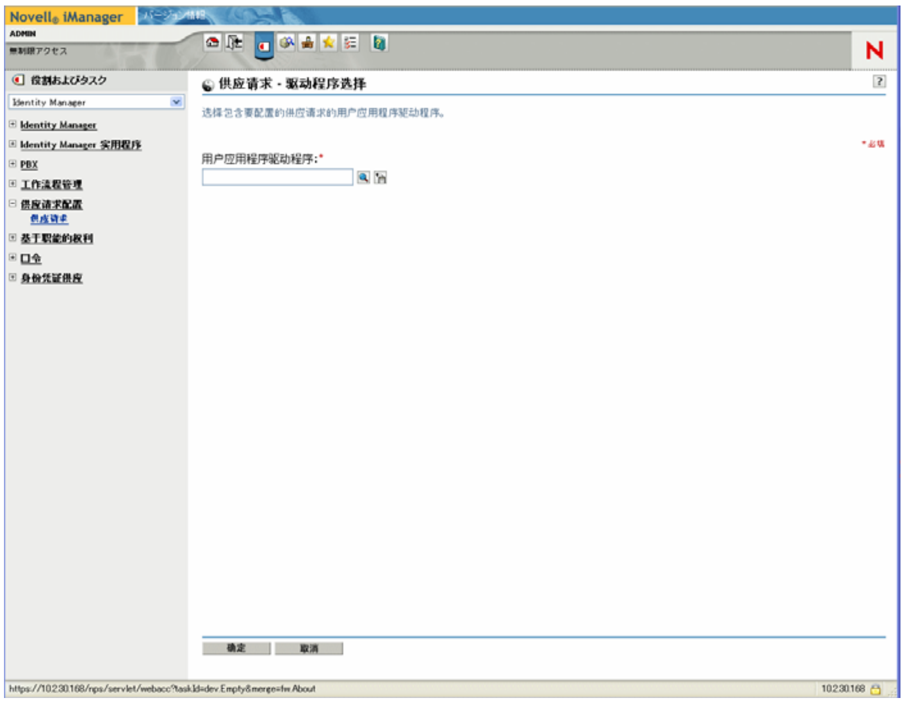
配置供应请求定义之前，需要选择包含该定义的 Identity Manager 用户应用程序驱动程序。选择了驱动程序之后，即可创建新的供应请求定义或编辑现有定义。还可以删除供应请求定义、更改请求定义的状态或定义请求定义的权限。

22.3.1 选择驱动程序

要选择 Identity Manager 用户应用程序驱动程序，请执行以下操作：

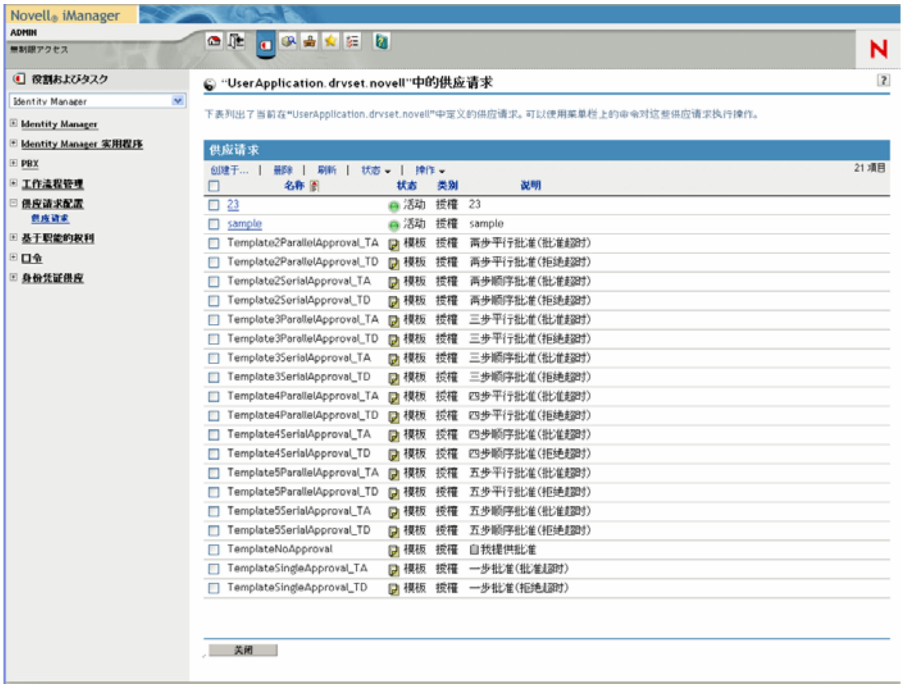
1. 在 iManager 中选择 *Identity Manager* 类别。
2. 打开 《供应请求配置》职能。
3. 单击 《供应请求》任务。

   iManager 即显示 《用户应用程序驱动程序》屏幕。



4. 在 《用户应用程序驱动程序》字段中指定驱动程序名称，然后单击 《确定》。

iManager 即显示 《供应请求配置》面板。 《供应请求配置》面板显示了可用的供应请求定义列表。



已安装的模板以黑色文本出现，其状态为 《模板》。如果请求定义是模板，将不显示超文本链接，因为它们是只读的。

注释 **:** 如果请求定义配置为使用经过本地化的文本，这些定义的名称和说明将显示适用于当前区域设置的文本。

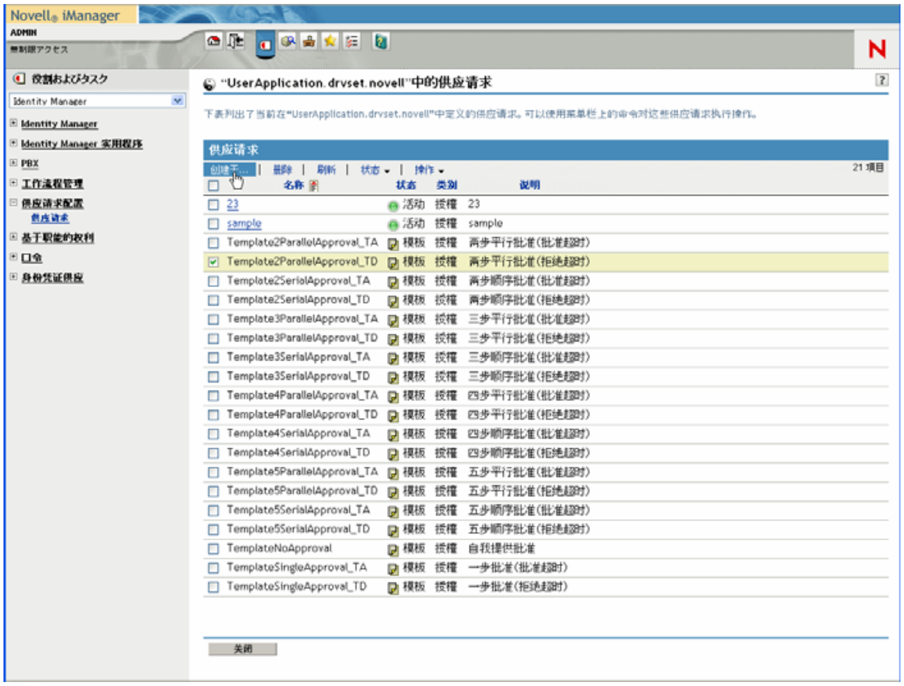
更改驱动程序 选择驱动程序后，除非选择新的驱动程序，否则所做的驱动程序选择在 iManager 会话期间将一直有效。要选择新的驱动程序，请单击 《操作》命令，然后从 《操作》菜单中选择 《选择用户应用程序驱动程序》。

22.3.2 创建或编辑供应请求

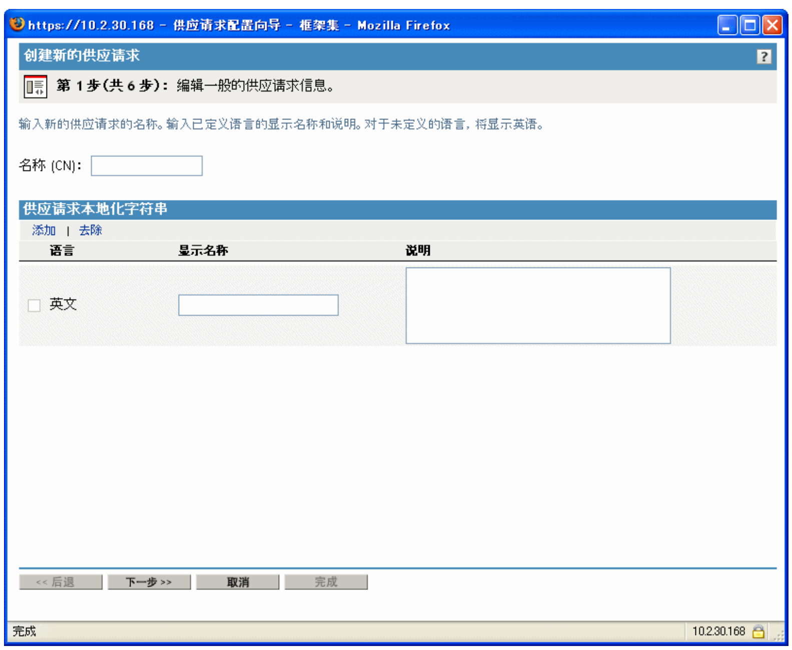
要创建新的供应请求，请执行以下操作：

1 在 《供应请求配置》面板中单击希望作为模板的供应请求的名称。

2 单击 《供应请求配置》面板中的 《创建于》命令。



即显示 《配置新的供应请求》向导的首页。



3 在 《名称》字段中键入新对象的常用名。

4 对于希望此应用程序支持的每种语言，请在 《供应请求本地化字符串》下面的 《显示名称》和 《说明》字段中键入本地化文本。该文本将在整个用户应用程序中用于标识此供应请求。

5 要向列表添加新的语言，请单击 《添加》并选择所需语言。

注释 : 默认情况下，新创建的供应请求仅支持英语。

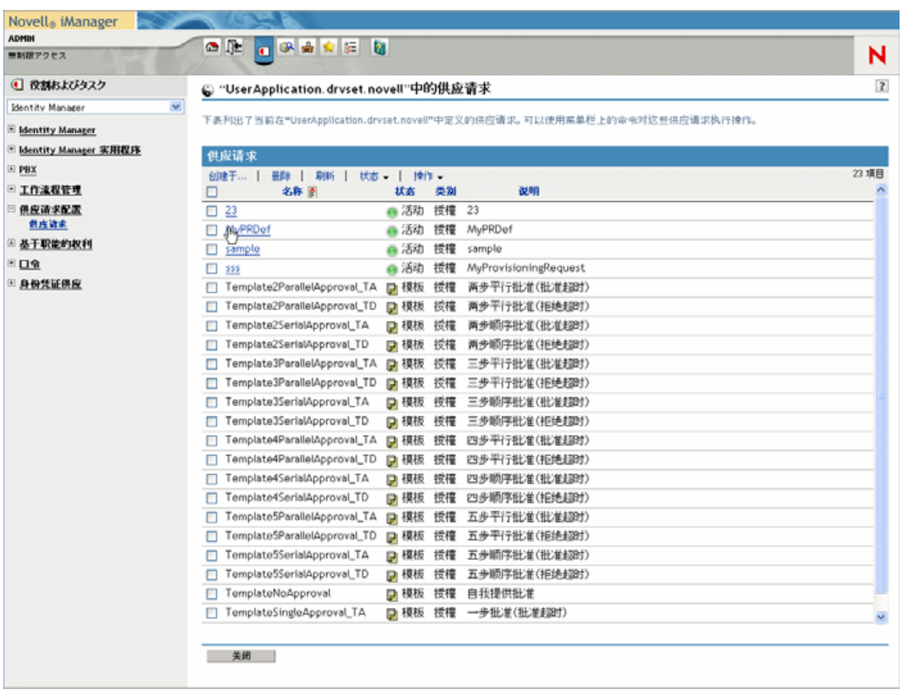
6 单击 《下一步》。
7 按照 “指定受供资源”在第 303 页 中的描述，指定请求定义的受供资源。
8 按照 “配置工作流程活动”在第 307 页 中的描述，配置与请求定义关联的工作流程的活动。
9 按照 “指定供应请求的访问权限”在第 310 页 中的描述，指定请求定义的访问权限。
10 按照 “指定供应请求的初始状态”在第 311 页 中的描述，指定请求定义的初始状态。

11 检查设置，并单击 《完成》。



要编辑现有供应请求，请执行以下操作：

1 在 《供应请求配置》面板中单击供应请求的名称。



不允许编辑用作模板的供应请求。状态为 《模板》的请求定义不显示超文本链接，因为它们是只读的。

注释：如果存在大量的请求定义，可能希望按特定列对列表进行排序，例如按《名称》或《说明》列进行排序。要按特定列排序，只需单击该列的标题。

2 在《供应请求本地化字符串》下面的列表中，选中希望此应用程序支持的语言旁边的复选框，并在《显示名称》和《说明》字段中键入本地化文本。该文本将在整个用户应用程序中用于标识此供应请求。
3 要向列表添加新的语言，请单击《添加》并选择所需语言。

注释：默认情况下，新创建的供应请求仅支持英语。

4 单击《下一步》。
5 按照“指定受供资源”在第 303 页中的描述，指定请求定义的受供资源。
6 按照“配置工作流程活动”在第 307 页中的描述，配置与请求定义关联的工作流程的活动。
7 按照“指定供应请求的访问权限”在第 310 页中的描述，指定请求定义的访问权限。
8 按照“指定供应请求的初始状态”在第 311 页中的描述，指定请求定义的初始状态。
9 检查设置，并单击《完成》。

指定受供资源

本节提供有关指定基于权利的受供资源的说明。它不提供有关权利的概念信息或创建和使用权利的说明。

有关权利的完整详细信息，请参见《*<z-DocTitleInVariable>Novell Identity Manager*：管理指南》。

要指定受供资源，请执行以下操作：

1 要使用当前与请求定义关联的目标，请选择《受供资源》单项选择按钮。

   如果正在编辑引用有效资源的请求定义，则默认情况下，已选中受供资源单项选择按钮。如果正在定义新的供应请求，则未选中此单项选择按钮。

2 要将请求定义联结到之前在当前选定的驱动程序中定义的其它资源，请选择 《可用的受供资源》单项选择按钮，并从下拉列表中选择一个目标。



注释 : 如果请求定义联结到不是权利的资源，则不允许更改此资源。

3 在 《类别》下拉列表中选择受供资源定义的类别。

类别默认为当前所选受供资源的类别。只要更改受供资源，也将更改请求定义的类别以与资源的类别相匹配。如果希望为请求定义指派一个不同的类别，请在 《类别》下拉列表中选择该类别。

4 要基于 Identity Manager 权利创建新资源，请单击 + 按钮。



要编辑现有资源，请单击此笔形按钮。



要定义资源的特征，请遵循以下步骤：

4a 在 《名称 (CN)》字段中指定资源的名称。

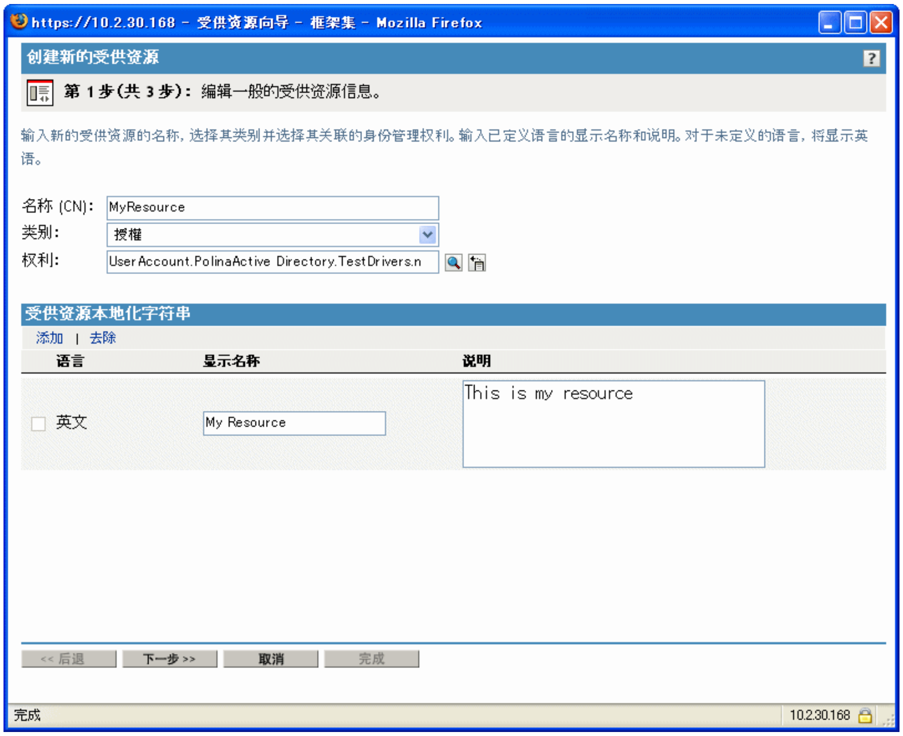
4b 在 《类别》下拉列表中选择资源的类别。

4c 在 《权利》字段中指定权利。

4d 在 《受供资源本地化字符串》下面的列表中，选中希望此应用程序支持的语言旁边的复选框，并在 《显示名称》和 《说明》字段中键入本地化文本。该文本将在整个用户应用程序中用于标识该供应资源。

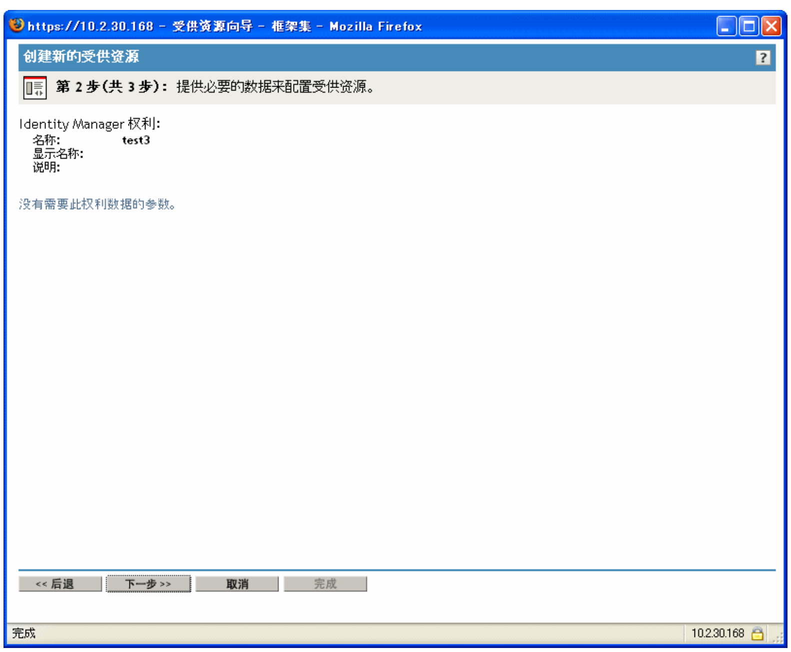
4e 要向列表添加新的语言，请单击 《添加》并选择所需语言。

注释 : 默认情况下，新创建的供应资源仅支持英语。



5 单击 《下一步》。

《受供资源》向导即显示一个屏幕，可以在其中为权利所需的任何参数提供数据。



6 如果此权利不需要任何权利参数，请单击 《下一步》。

《创建新的受供资源》向导即显示 《摘要》页，该页提供正在定义的资源的信息。

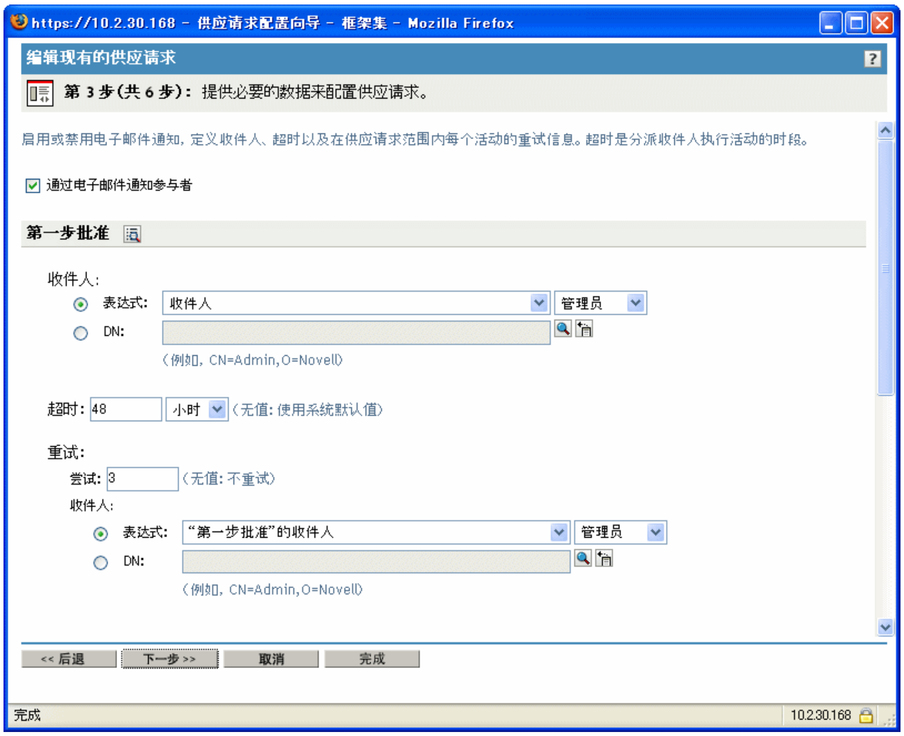


7 单击 《完成》。

配置工作流程活动

要配置关联工作流程的活动，请执行以下操作：

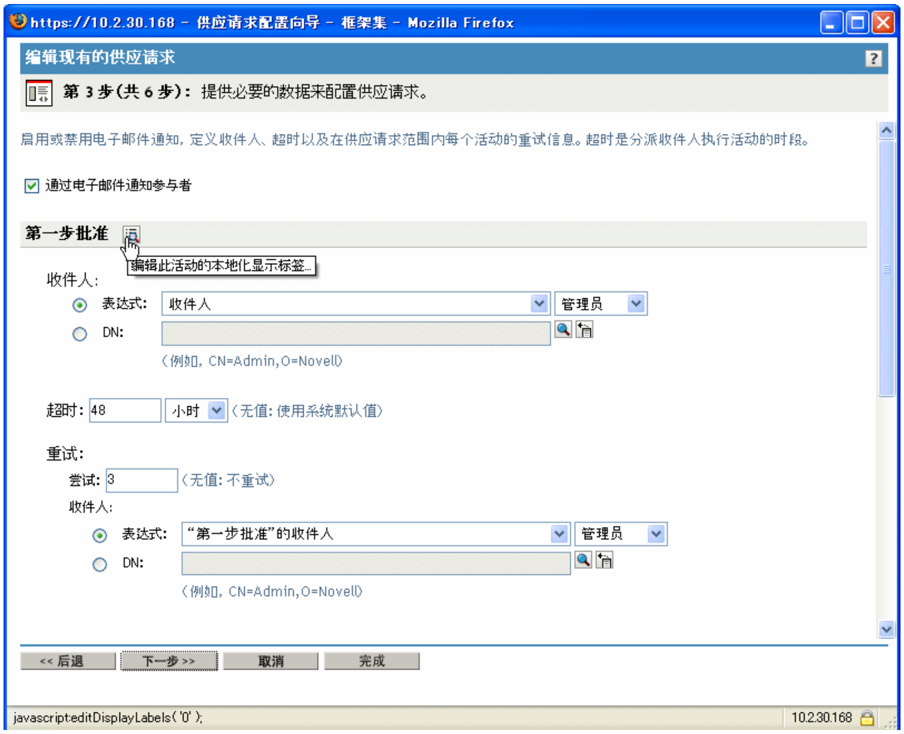
1 通过选中或取消选中 *Notify participants by e-mail* （通过电子邮件通知参与者）复选框，指定是否想通过电子邮件通知每项活动的收件人。



注释 **:** 如果选中 《通过电子邮件通知参与者》复选框，并且收件人指定了一个代理，那么也会通过电子邮件通知该代理。但不会通过电子邮件通知受托人。

---

2 通过单击工作流程活动名称旁边的图标，可更改每项活动的显示标签 （在本例中为《第一步批准》），这一操作是可选的。



在 《显示标签》字段中键入显示标签并单击 《确定》。



注释 : 默认显示标签 （《第一步批准》、《第二步批准》等）表明批准是按顺序处理的。对于并行流程，可能希望指定不按顺序处理的标签。例如，可能想要指派三个并行批准中的一个批准，三个并行批准中的两个批准等标签。

3 另外还为每项工作流程活动提供了以下信息：

字段	说明
收件人表达式	指定标识活动收件人的动态表达式。在运行时根据此表达式的求值方式确定收件人。 收件人表达式的**第一项**可为以下任意值： ◆ Initiator （发起人） ◆ Recipient （收件人） ◆ Addressee of *activity-name* （活动名称的收件人） 对于工作流程中的每项活动 （当前正配置的活动除外），都会在《表达式》下拉列表中单独列出一个*活动名称* 的收件人项。*活动名称* 是为此项活动指定的显示标签，如果没有指定显示标签，该名称即为默认名称。 收件人表达式的**第二项**可以为以下任一值： ◆ Manager ◆ <No attribute> **注释 :** Manager 特性自动可用，因为先前已经在提取层中的用户实体上定义过它。其它特性 （Manager 除外）如果符合以下要求，也可供选择： ◆ 必须在提取层中的用户实体上定义 ◆ 必须为单值 ◆ 必须有 DN 数据类型
收件人 DN	为用户、组或任务组指定判别名。 **注释 :** 如果希望任务组管理员能按任务组搜索任务 （在用户应用程序中的 《我的小组任务》操作中），需要将任务组指定为收件人。
超时	指定分配给收件人完成任务的时间段。每次收件人执行活动时，都会应用超时间隔。 以秒、分钟、小时或天为单位指定一个值。
重试	指定在超时情况下重试活动的次数。 活动超时后，工作流程进程可能会试图再次完成该活动，这取决于为该活动指定的重试计数。每次重试时，工作流程进程可能会将活动上报给另一用户。在此情况下，会将该活动重指派给其他收件人 （例如，该用户的经理），使该用户还有机会完成该活动的工作。如果最后一次重试超时，则可能会将该活动标记为已批准或已拒绝，这取决于工作流程的配置。

字段	说明
重试收件人表达式	指定一个动态表达式，该表达式用于确定在达到超时限制时应获得此任务的用户。 在运行时根据该表达式的求值方式确定重试收件人。 收件人表达式的**第一项**可为以下任意值： ◆ approval.getAddressee() ◆ Initiator （发起人） ◆ Recipient （收件人） ◆ Addressee of *activity-name* （活动名称的收件人） approval.getAddressee() 选项获取当前收件人。 对于工作流程中的每项活动 （包括当前正配置的活动），都会在 《表达式》下拉列表中单独列出一个*活动名称* 的收件人项。*活动名称* 是为此项活动指定的显示标签，如果没有指定显示标签，该名称即为默认名称。 收件人表达式的**第二项**可以为以下任一值： ◆ Manager ◆ <No attribute> 如果选择 approval.getAddressee() 选项，然后选择 Manager，则每次重试都将上报至组织内更高级别的新经理。因此，需要确保设置适合于组织的重试计数。在任何情况下，重试计数都不应超过当前收件人之上管理级别的数目。
重试收件人 DN	指定在达到重试限制的情况下应获得此任务的用户或组的判别名。

4 配置完活动后，可能需要向下滚动以查看此流程的其它活动。

5 单击 《下一步》。

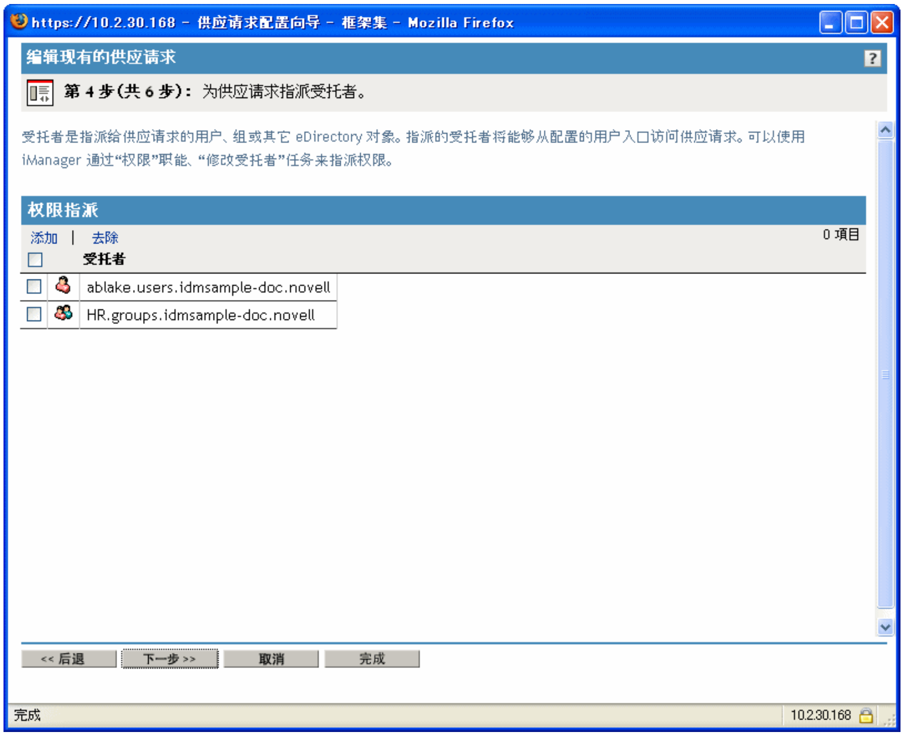
注释 **:** 可以配置的活动数量取决于联结到请求定义的工作流程模板。权利参数的数量和类型取决于与请求关联的受供资源。

指定供应请求的访问权限

要指定供应请求的访问权限，请执行以下操作：

1 要向此请求定义的受托者列表添加用户、组或其它 eDirectory 对象，请单击 《添加》并选择此对象。

添加对象后，该对象会包括在受托者列表中。



2 要去除用户、组或其它对象，请在 《受托者》列表中选择该项目并单击 《去除》。

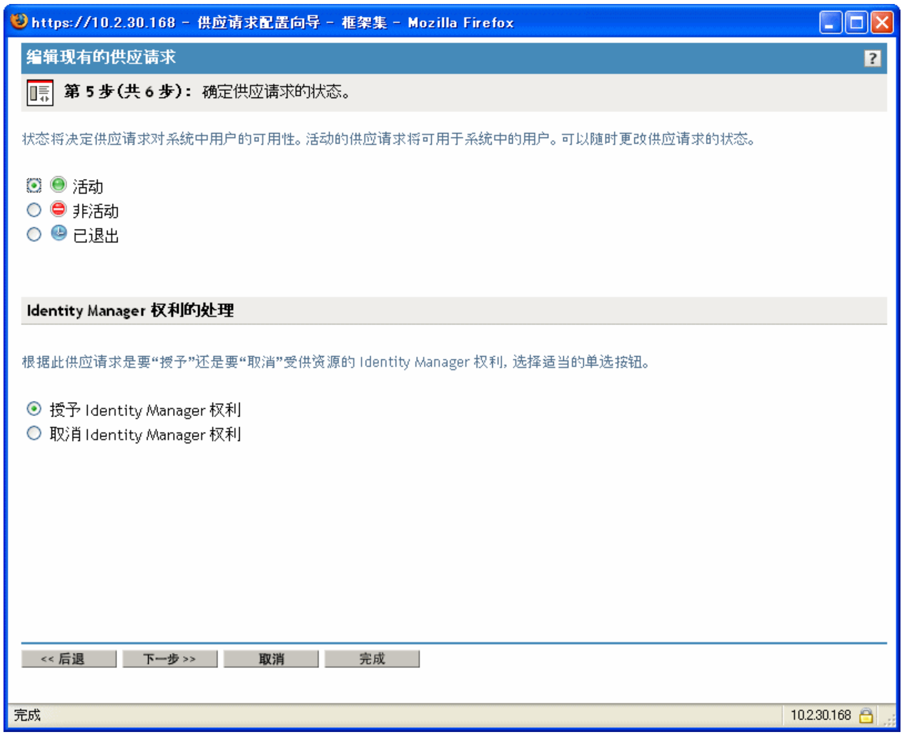
3 单击 《下一步》。

指定供应请求的初始状态

要设置供应请求的初始状态，请执行以下操作：

1 单击所需状态的单项选择按钮：

状态	说明
活动的	可用。
不活动的	暂时不可用。此为默认设置。
已退出	永久禁用。



2 单击正确操作的单项选择按钮 （授予或撤消）。

3 单击 《下一步》。

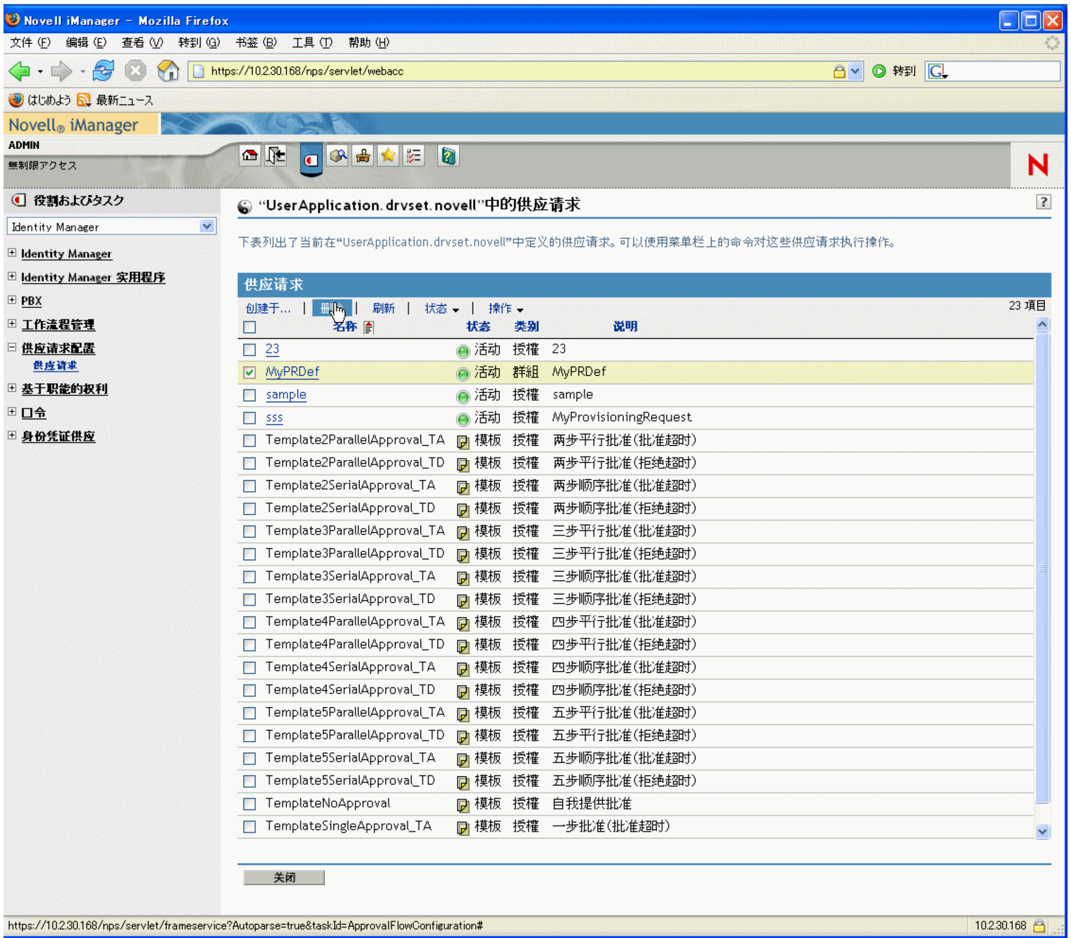
22.3.3 删除供应请求

要删除供应请求，请执行以下操作：

1 选择要删除的供应请求，方法是单击其名称旁的复选框。

不允许删除作为模板的供应请求。

2 单击 《供应请求配置》面板中的 《删除》命令。

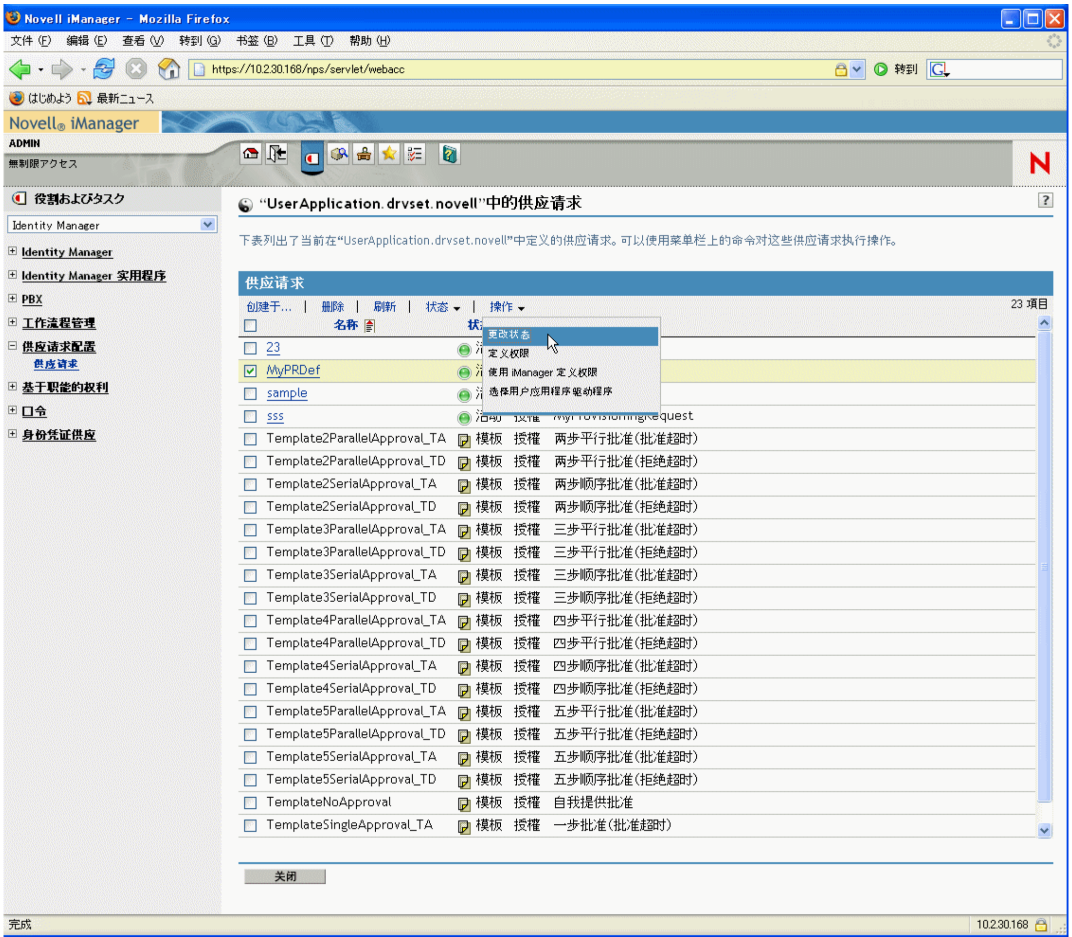


22.3.4 更改现有供应请求的状态

要更改现有供应请求的状态，请执行以下操作：

1 选择要更改状态的供应请求，方法是单击其名称旁的复选框。

2 单击 《供应请求配置》面板中的 《更改状态》命令。



3 单击 《状态》菜单中的状态：

状态	说明
活动的	可用。
不活动的	暂时不可用。
已退出	永久禁用。

4 单击正确操作的单项选择按钮 （授予或撤消）。

5 单击 《完成》。

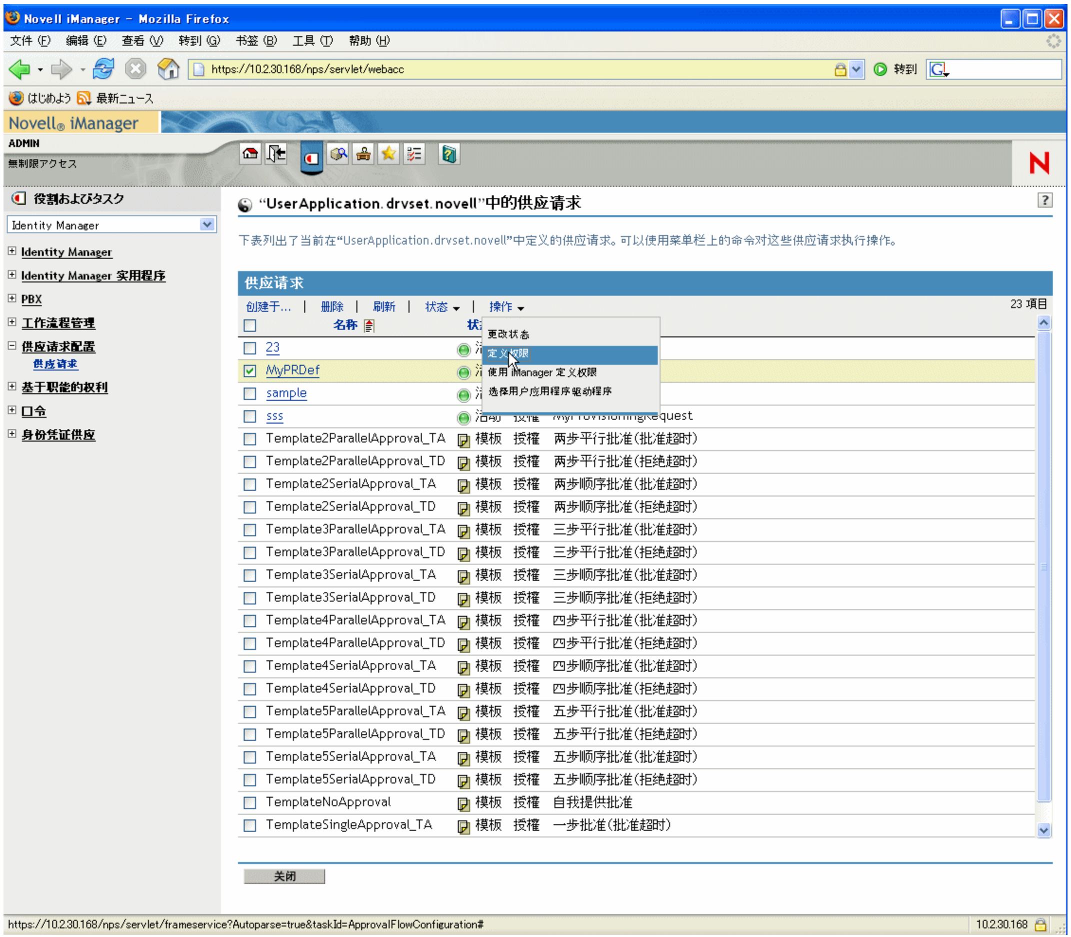
22.3.5 定义对现有供应请求的权限

要定义对现有供应请求的权限，请执行以下操作：

1 选择要定义权限的供应请求，方法是单击其名称旁的复选框。

2 单击 《供应请求配置》面板中的 《操作》命令。

3 单击 《操作》菜单中的 《定义权限》命令。



4 请按 "指定供应请求的访问权限" 在第 310 页 中提供的步骤进行操作。

要使用 iManager 定义对供应请求的权限，请执行以下操作：

1 选择要定义权限的供应请求，方法是单击其名称旁的复选框。

2 单击 《供应请求配置》面板中的 《操作》命令。

3 单击 《操作》菜单上的 《使用 iManager 定义权限》命令。

管理供应工作流程 23

本章提供了在运行时管理供应工作流程的说明。还提供了为供应工作流程配置电子邮件通知的说明。

包括以下主题：

23.1 关于工作流程管理插件

iManager 的工作流程管理插件提供了一个基于浏览器的界面，可通过该界面查看工作流程进程的状态，重指派工作流程内的活动或在工作流程停止时终止它。

可以在 iManager 中的 *Identity Manager* 类别中找到工作流程管理插件。此插件包括 《工作流程管理》职能中的 《工作流程》任务。

《工作流程管理》职能还包括 《电子邮件模板》和 《电子邮件服务器选项》任务。这些任务是 《口令》职能下列出的其它任务的快捷方式。

关于工作流程任务 工作流程任务包含以下面板：

面板	说明
工作流程	提供用于管理供应工作流程的主要用户界面。该界面列出了当前正在处理的工作流程，并允许对这些工作流程执行各种操作。 首次启动工作流程任务时，工作流程面板要求选择一个 Identity Manager 用户应用程序驱动程序。该驱动程序指向工作流程服务器。需要先选择一个驱动程序，然后才能登录服务器并开始管理工作流程。 选择驱动程序后，可以指定搜索准则以选择要管理的工作流程。
工作流程细节	提供一个只读的用户界面，用于查看有关特定工作流程的细节。

23.2 管理工作流程

本节包括使用工作流程管理插件管理供应工作流程的步骤。

23.2.1 连接到工作流程服务器

开始管理工作流程之前，需要连接到工作流程服务器。如果将用户应用程序驱动程序联结到一个工作流程服务器，则只需指定要使用的驱动程序名称。如果该驱动程序与多个工作流程服务器关联，则需要选择目标工作流程服务器。

要连接到工作流程服务器，请执行以下操作：

1 在 iManager 中选择 Identity Manager 类别。

2 打开 《工作流程管理》职能。

3 单击 《工作流程》任务。

iManager 将显示 《工作流程》屏幕。

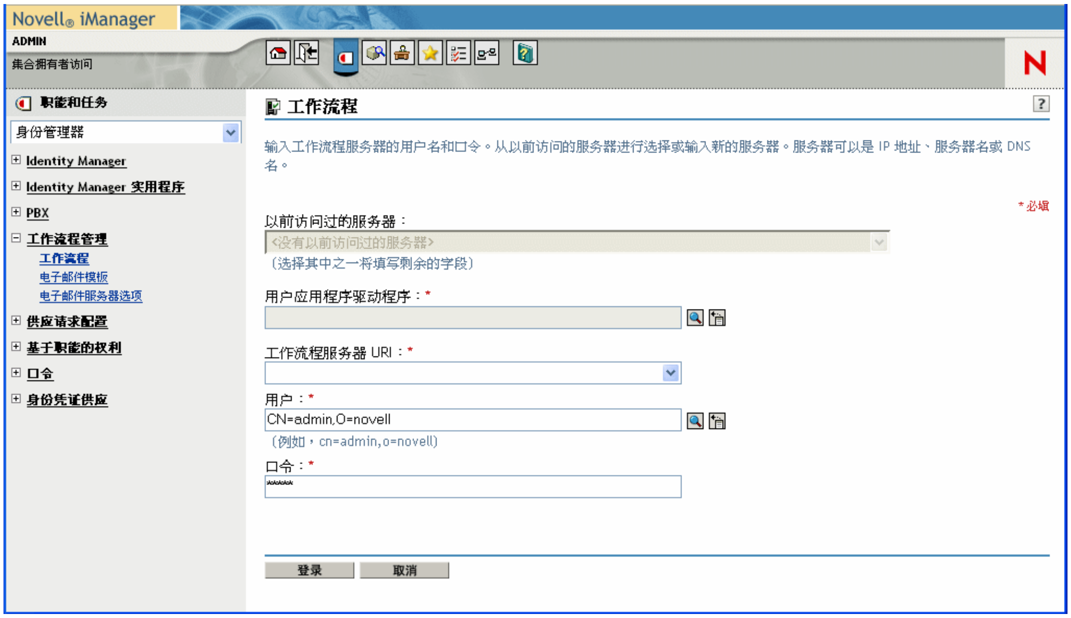


4 如果以前访问过目标工作流程服务器，则可以从 《以前访问过的服务器》下拉列表中选择此服务器。

iManager 会填充屏幕中的其余字段。

5 如果尚未访问过工作流程服务器，请在 《用户应用程序驱动程序》字段中指定驱动程序名称并单击 《确定》。

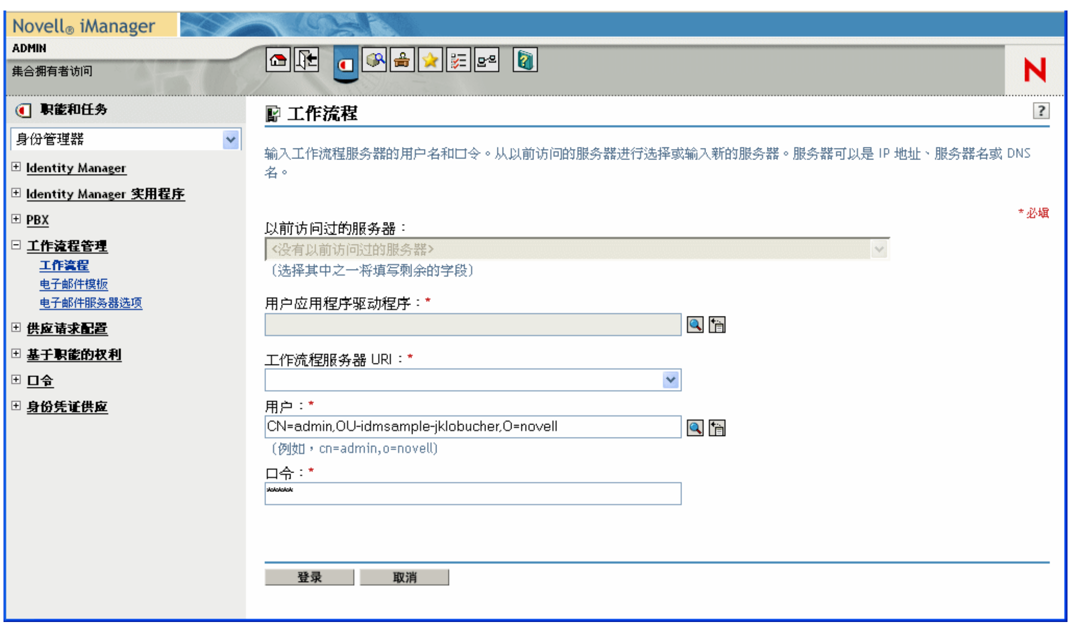
iManager 会填充屏幕中的其余字段。



6 如果此驱动程序与多个工作流程服务器关联，请在 《工作流程服务器 URI》字段中选择目标服务器。

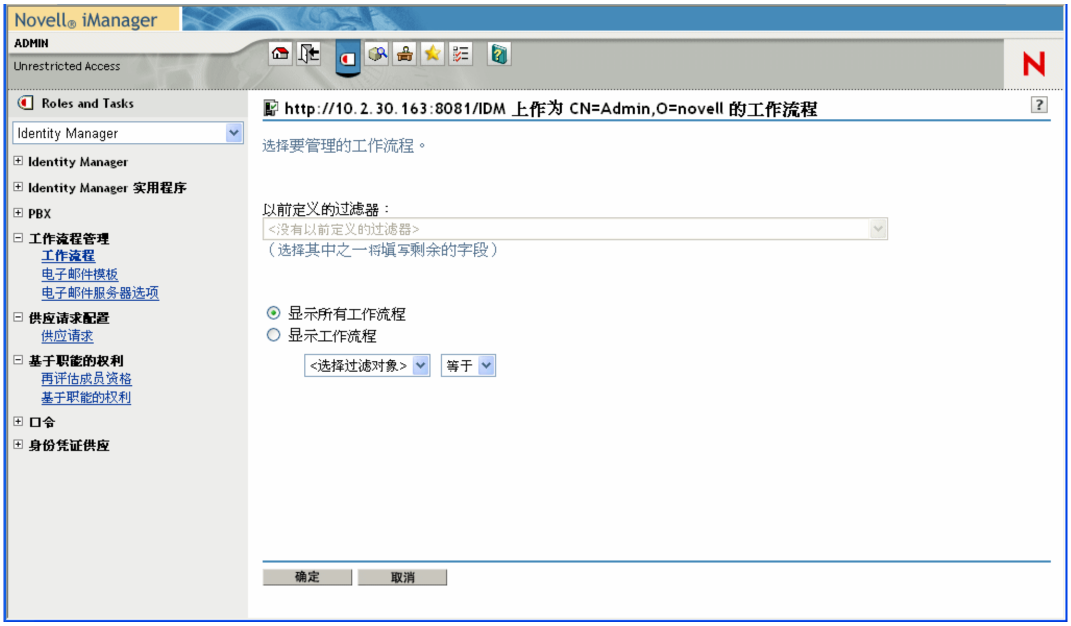
7 还可以选择替换 《用户》字段中的用户名和 《口令》字段中的口令。

该用户必须是用户应用程序管理员。默认情况下，用户名设置为当前登录到 iManager 的用户。如果该用户不是管理员，则需要更改用户名。例如，可能希望修改用户以指向 idmsample 测试 OU 的用户应用程序管理员，如下所示：



8 单击 《登录》。

工作流程管理插件显示一个页面，用于指定一个过滤器以查找工作流程：



23.2.2 查找与搜索准则匹配的工作流程

如果目标工作流程服务器正在运行大量的工作流程进程，可能需要过滤在 iManager 中看到的工作流程列表。要进行此操作，可以指定搜索准则。

要指定用于过滤工作流程列表的搜索准则，请执行以下操作：

1 选择 《显示工作流程》单项选择按钮。



注释：默认情况下，已选择《显示所有工作流程》单项选择按钮。如果要查看服务器上工作流程的完整列表，请不要更改默认设置。

2 选择要为其指定准则的特性。

特性	说明
Creation time （创建时间）	启动工作流程的时间。
Initiator （发起人）	请求者的用户名。
Recipient （收件人）	收件人的用户名。
Process Status （进程状态）	工作流程进程的整体状态 （已完成、正在运行或已终止）。
Approval status （批准状态）	批准进程的状态 （已批准、被拒绝或已收回）。
Entitlement status （权利状态）	由供应请求启动的权利的状态 （错误、致命、成功、未知或警告）。

3 选择运算符：

运算符	注释
等于	支持所有特性。
之前	仅支持 Creation time 特性。
之后	仅支持 Creation time 特性。
之间	仅支持 Creation time 特性。

4 在特性和运算符下面的字段中指定一个值。

对于创建时间，可以使用《日期和时间》控件选择值。对于发起人和收件人，可以使用《对象历史》或《对象选择器》指定值。对于所有其它特性，请从下拉列表中选择值。

5 单击《确定》。

iManager 会在 《工作流程》面板中显示所选择的工作流程。



更改目标服务器和过滤器 选择工作流程服务器之后，所选的服务器在 iManager 会话期间始终有效，除非选择了新服务器。若要选择新的服务器，请单击 《操作》命令并从 《操作》菜单中选择 《选择服务器》。



要指定不同的搜索准则，请在 《操作》菜单中选择 《定义过滤器》。



23.2.3 控制活动工作流程的显示

《工作流程》面板列出了与指定的搜索准则匹配的工作流程。除了过滤此列表外，还可以控制显示。例如，可以指定刷新列表和按特定列排序列表的频率。

刷新工作流程的列表

工作流程服务器很忙时，活动工作流程的列表可能会频繁地更改。在这种情况下，需要刷新在服务器上运行的活动工作流程的列表。

要刷新工作流程的列表，请执行以下操作：

1 单击 《工作流程》面板中的 《刷新》命令。

2 通过从 《刷新》菜单中选择以下选项之一，指定要使用的刷新间隔：

2a 刷新关闭

2b 立刻刷新

2c 10 秒

2d 30 秒

2e 60 秒

2f 5 分钟

排序工作流程的列表

如果存在大量的请求定义，可能希望按特定列对列表进行排序，例如按 《名称》或 《说明》列进行排序。

要排序工作流程列表，请执行以下操作：

1 单击排序列的标题。

23.2.4 终止工作流程实例

如果不希望工作流程实例继续处理，可以终止该工作流程。

要终止工作流程进程实例，请执行以下操作：

1 在 《工作流程》面板中，单击工作流程名称旁的复选框以选择该工作流程。
2 单击 《工作流程》面板中的 《终止》命令。

23.2.5 查看有关工作流程实例的细节

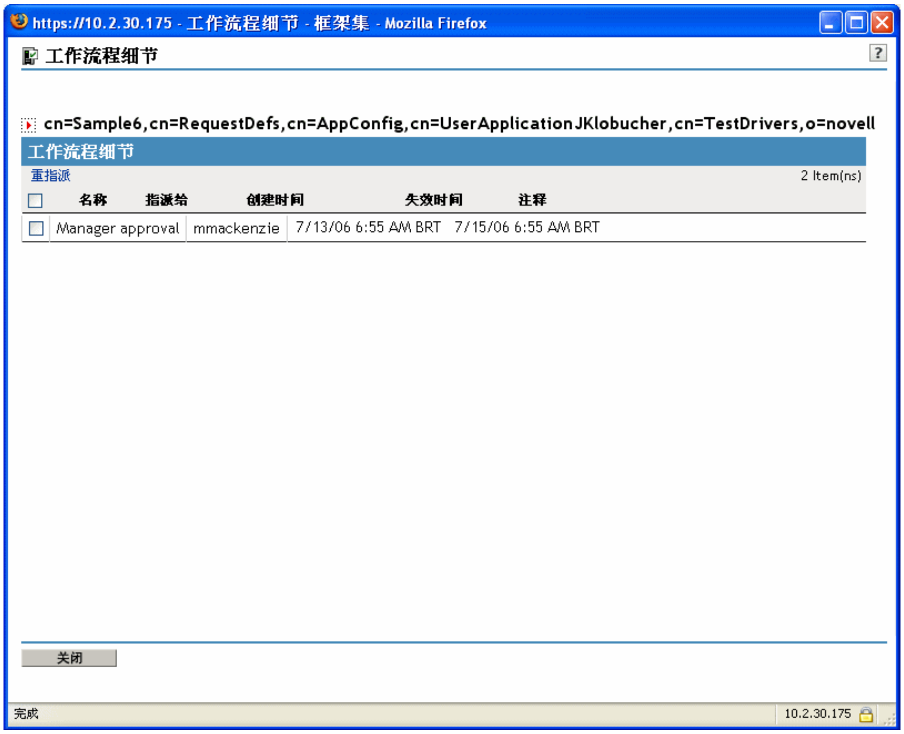
在特定服务器上显示一组正在运行的工作流程之后，可以选择工作流程实例以查看有关正在运行的进程的更多细节。

注释 : 如果工作流程实例使用串行处理设计模式，则只将一个活动显示为当前活动，因为在任何时间点只有一个用户可以操作该工作项目。但是，如果工作流程进行并行处理和分支，则一个工作流程实例可能有多个当前活动。

要查看有关特定工作流程实例的细节，请执行以下操作：

1 在 《工作流程》面板中单击工作流程实例的名称。

iManager 会显示 《工作流程细节》面板。



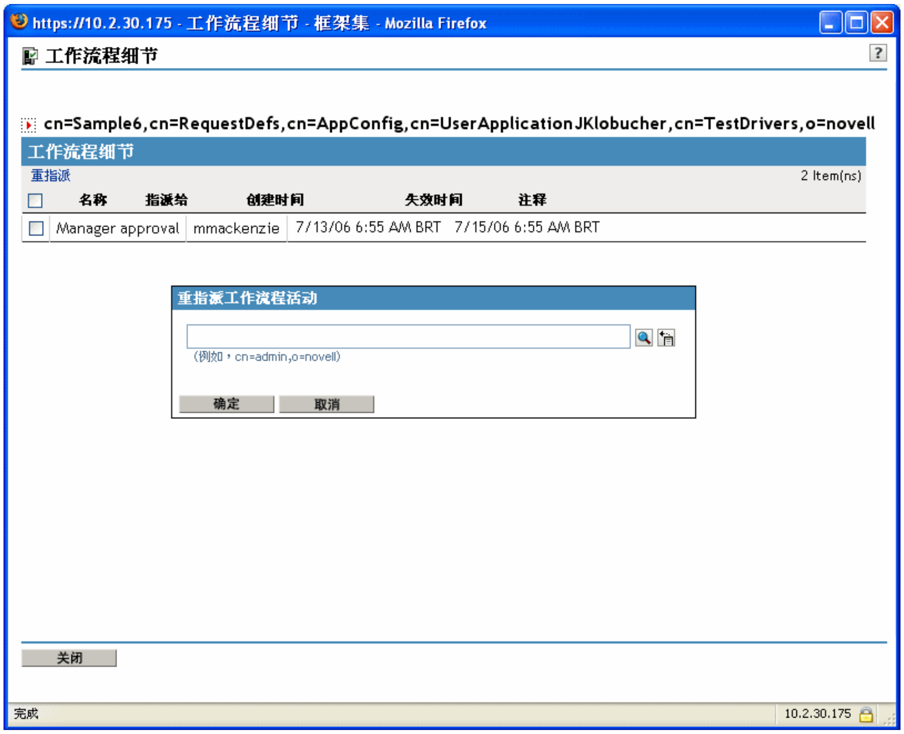
23.2.6 重指派工作流程实例

如果工作流程实例停止，可以将此工作项目重指派给其它用户或组。

要重指派工作流程实例，请执行以下操作：

1 选择与此工作流程关联的当前活动，方法是在 《工作流程细节》面板中单击其名称旁的复选框。

2 单击 《工作流程细节》面板中的 《重指派》命令。



3 选择要为此工作项目重指派的用户或组。

23.3 配置电子邮件服务器

工作流程进程通常会在执行过程中的多个时刻发送电子邮件通知。例如，将一个工作流程活动指派给一个新收件人时，可能会发送电子邮件。

需要先配置 SMTP 电子邮件服务器，然后才能利用 Identity Manager 的电子邮件通知功能。为此，需要使用 iManager 中 《工作流程管理》职能中的 《电子邮件服务器选项》任务。

注释 **:** 此任务是 《口令》职能下 《电子邮件服务器选项》任务的快捷方式。

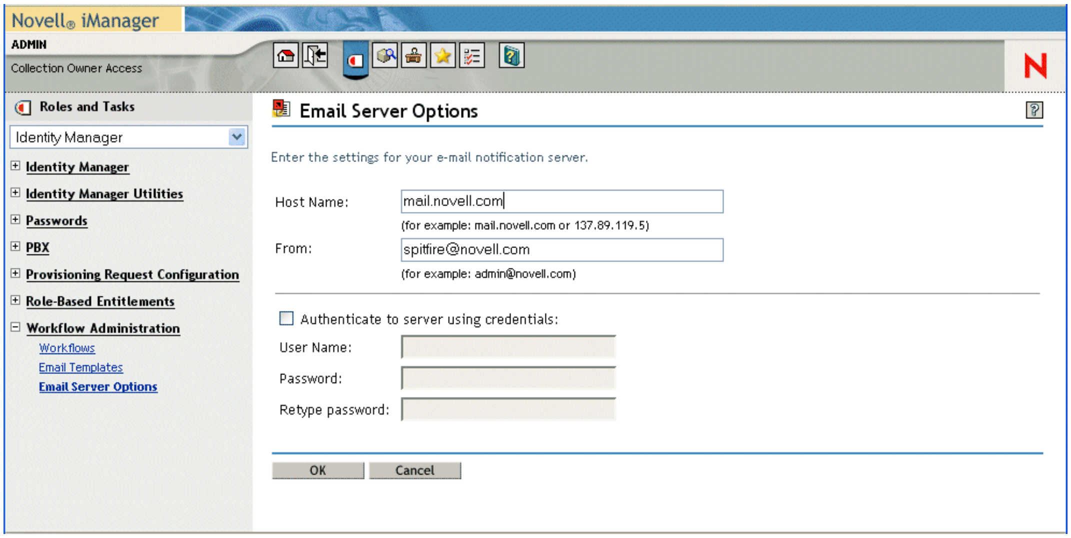
要配置电子邮件服务器，请执行以下操作：

1 在 iManager 中选择 Identity Manager 类别。

2 打开 《工作流程管理》职能。

3 单击 《电子邮件服务器选项》任务。

iManager 即显示 《电子邮件服务器选项》屏幕。



4 在 《主机名》字段中，键入主机服务器的名称 （或 IP 地址）。

5 在 《发件人》字段中，键入寄件人的电子邮件地址。

收件人打开电子邮件时，此文本将显示在电子邮件标题的 《发件人》字段中。根据邮件服务器设置，该字段中的文本可能需要与系统中有效的寄件人匹配，以允许邮件服务器进行反向查找或鉴定。例如，可以是 helpdesk@company.com，而不是 《口令管理员》之类的描述性文本。

6 如果服务器在发送电子邮件之前需要进行鉴定，请选中 《使用身份凭证鉴定到服务器》复选框并指定用户名和口令。

7 完成后，请单击 《确定》。

23.4 使用安装的电子邮件模板

Identity Manager 附带了一个专为基于工作流程的供应设计的电子邮件模板。此电子邮件模板称为新的供应请求。该产品附带的所有供应请求模板均与此电子邮件模板关联。因此，所创建的任何新请求定义都将使用此电子邮件模板。

可以编辑 《新的供应请求》模板以更改电子邮件讯息的内容和格式，但无法创建新的电子邮件模板。

要编辑 《新的供应请求》模板，需要使用 iManager 中 《工作流程管理》职能中的 《电子邮件模板》任务。

注释 **:** 此任务是 《口令》职能下 《编辑电子邮件模板》任务的快捷方式。

23.4.1 默认内容和格式

安装此产品之后，《新的供应请求》模板的外观如下所示：

```
Dear $userFirstName$, A new provisioning request has been submitted
```

```
that requires your approval. Request name: $requestTitle$ Submitted
by: $initiatorFullName$ Recipient: $recipientFullName$ Please review
the details of this request at $PROTOCOL$://$HOST$:$PORT$/
$TASK_DETAILS$ to take the appropriate action. You can review a list of
all requests pending your approval at $PROTOCOL$://$HOST$:$PORT$/
$TASKLIST_CONTEXT$.
```

该模板标识了触发此电子邮件讯息的供应请求定义。此外，它还包括两个 URL，一个可将收件人重定向到需要批准的任务，另一个可显示该用户的待处理任务的完整列表。

23.4.2 编辑模板

可以更改 《新的供应请求》模板的内容或格式。请注意，该模板应用于 Identity Manager 用户应用程序中的所有供应请求，因此请确保所做的编辑适用于所有用户和工作流程任务。

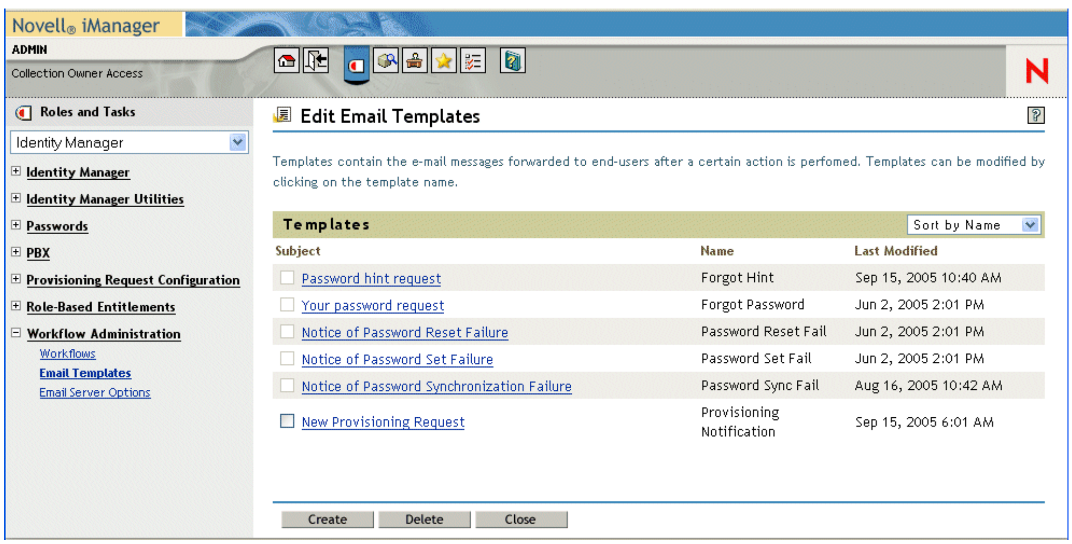
要编辑模板，请执行以下操作：

1 在 iManager 中选择 Identity Manager 类别。

2 打开 《工作流程管理》职能。

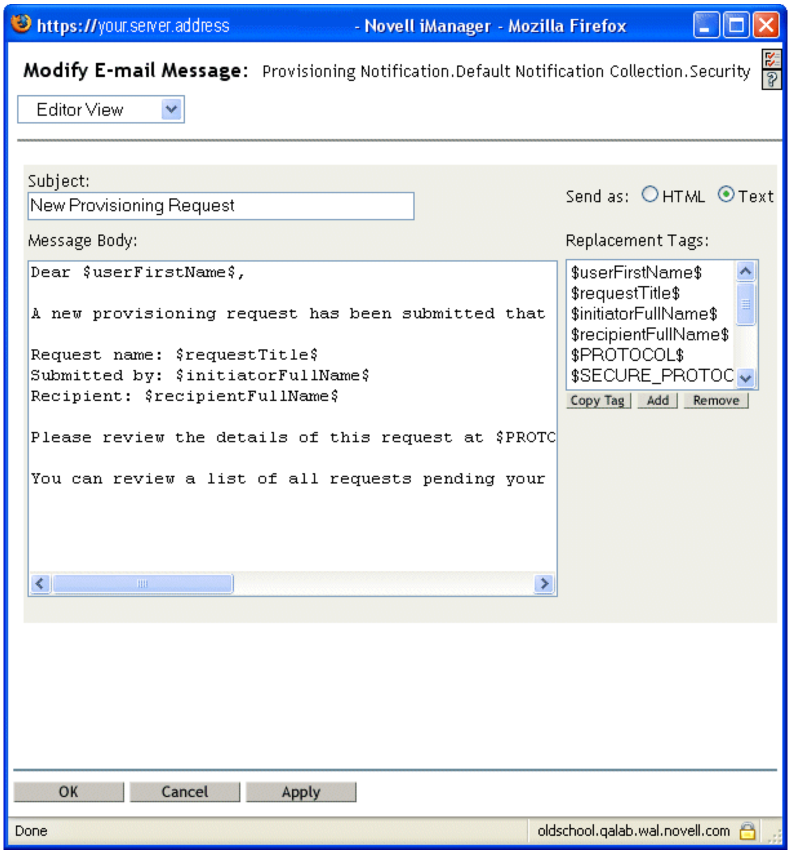
3 单击 《电子邮件模板》任务。

iManager 即显示 《编辑电子邮件模板》屏幕。



4 单击模板列表中的 《新的供应请求》。

iManager 即显示 《修改电子邮件讯息》屏幕。



5 请在 《讯息体》框中进行更改。

6 如果需要，可复制 《替换标记》列表框中的一个或多个标记，从而在讯息体中加入动态文本。

下面是这些替换标记的简要说明：

标记	说明
$userFirstName$	收件人的名。
$requestTitle$	供应请求定义的显示名称。
$initiatorFullName$	发起人的全名。
$recipientFullName$	收件人的全名。
$PROTOCOL$	电子邮件讯息中包含的 URL 的协议。
$SECURE_PROTOCOL$	电子邮件讯息中包含的 URL 的安全协议。
$HOST$	正在运行 Identity Manager 用户应用程序的 JBoss 应用程序服务器的主机。
$PORT$	Identity Manager 用户应用程序的端口。
$SECURE_PORT$	Identity Manager 用户应用程序的安全端口。
$TASKLIST_CONTEXT$	显示待发给收件人的所有请求列表的页。

标记	说明
$ 任务 _ $	显示请求 （此电子邮件讯息即为该请求生成）细节的页。

7 完成后，请单击 《确定》。

23.4.3 修改模板的默认值

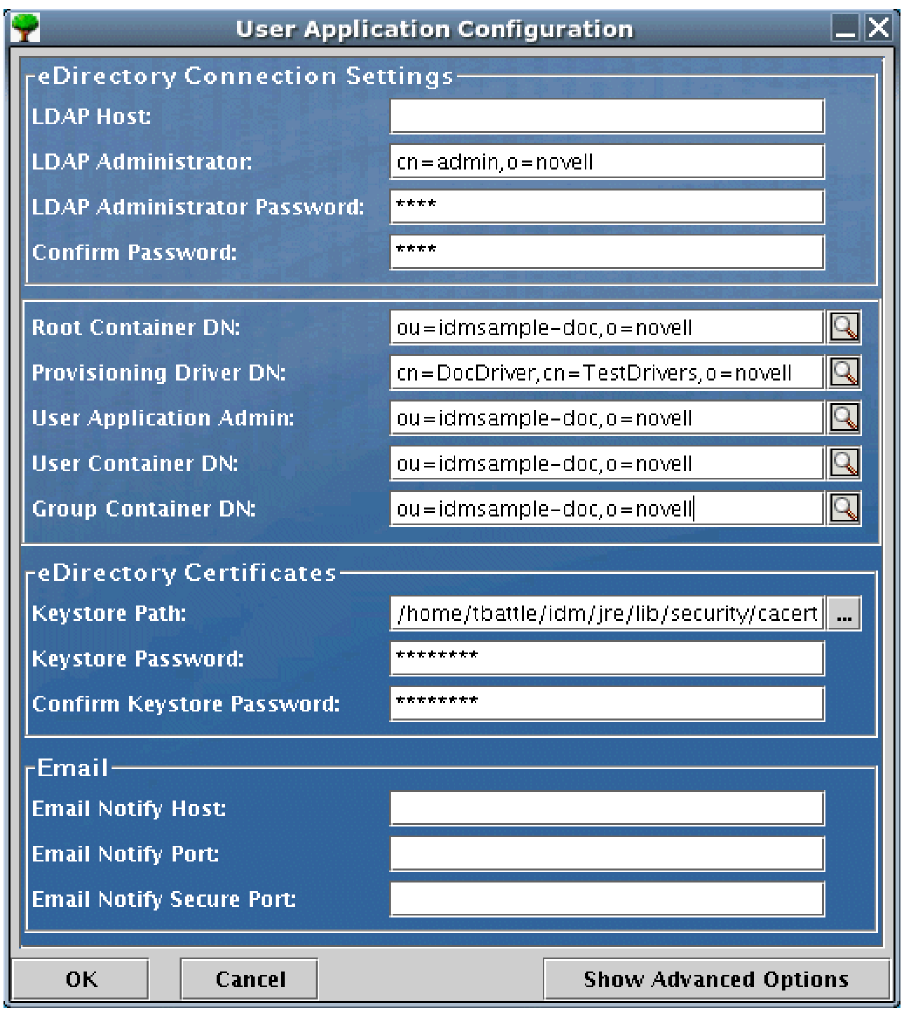
安装时，可以为电子邮件模板中使用的多个替换标记设置默认值。完成安装之后，还可以使用 《用户应用程序配置》工具修改这些值。

要修改这些安装设置，请执行以下操作：

1 运行 idm 文件夹中的 ldapconfig.sh 底稿。

```
./configupdate.sh
```

注释：在 Windows 中，要运行的文件为 configupdate.bat。



2 必要时可对以下任意字段进行更改：

字段	说明
电子邮件通知主机	用于替换批准流程中使用的电子邮件模板中的 $HOST$ 标记。如果保留为空白，则由服务器进行计算。（这是 JBoss 主机。）
电子邮件通知端口	用于替换批准流程中使用的电子邮件模板中的 $PORT$ 标记。
电子邮件通知安全端口	用于替换批准流程中使用的电子邮件模板中的 $SECURE_PORT$ 标记。

3 单击 《确定》确认更改。

附录 VI

以下附录提供了 Identity Manager 用户应用程序的其它参考信息和高级主题。

纲要扩展 A

A.1 特性纲要扩展

特性名称	说明
srvprvAOLIMAddress	**AOL IM 地址**
srvprvActiveDelegatees	用户的活动受托人
srvprvActiveDelegators	用户的活动委托者
srvprvAssetRef	命名资产 （通过 srvprvAssetRecipientAux 类与用户关联）的聚合资产属性的表示形式
srvprvAssignExpiration	代理或委托指派失效的时间
srvprvAssignFromContainer	代理或委托指派的树枝主题
srvprvAssignFromGroup	代理或委托指派的组主题
srvprvAssignFromUser	代理或委托指派的用户主题
srvprvAssignToRelationship	委托指派的目标关系
srvprvAssignToUser	代理或委托指派的用户目标
srvprvCategoryKey	将给定的供应请求定义与一组供应类别关联。值为 srvprvChoice 实例的键
srvprvDefaultTheme	默认主题
srvprvEntitlementRef	DirXML 权利参照
srvprvEntityType	指定目录提取层实体定义的类型
srvprvFlowStrategy	指定要用于供应请求定义的流程调用策略
srvprvGrant	一种标志，如果为 True，则指定供应请求定义支持授予操作
srvprvGroupwiseIMAddress	Groupwise IM 地址
srvprvHeaderFillerFile	标题填充文件名
srvprvHeaderFillerImage	标题填充图像
srvprvHeaderFillerLastMod	标题填充图像上次修改时间
srvprvHeaderLogo2File	标题徽标副图像文件名
srvprvHeaderLogo2Image	标题徽标副图像
srvprvHeaderLogo2LastMod	标题徽标副图像上次修改时间
srvprvHeaderLogoFile	标题徽标主图像文件名
srvprvHeaderLogoImage	标题徽标主图像

特性名称	说明
srvprvAOLIMAddress	**AOL IM 地址**
srvprvHeaderLogoLastMod	标题徽标主图像上次修改时间
srvprvHeaderTextureFile	标题纹理文件名
srvprvHeaderTextureImage	标题纹理图像
srvprvHeaderTextureLastMod	标题纹理图像上次修改时间
srvprvIsTaskManager	指示用户是否为任务组管理员
srvprvLocalizedDescrs	为供应万维网应用程序、设计程序和 iManager 提供经过本地化的说明字符串集
srvprvLocalizedNames	为供应万维网应用程序、设计程序和 iManager 提供经过本地化的显示名称字符串集
srvprvLoginFile	登录文件名
srvprvLoginImage	登录图像
srvprvLoginLastMod	登录图像上次修改时间
srvprvLoginSmallFile	登录小图像文件名
srvprvLoginSmallImage	登录小图像
srvprvLoginSmallLastMod	登录小图像上次修改时间
srvprvModified	一种标志，用于指示对目录模型树枝中的定义对象实例的更改
srvprvNavBckgrColor	导航背景色
srvprvNavBckgrColorLastMod	导航背景色上次修改时间
srvprvNavColor	导航颜色
srvprvNavColorLastMod	导航颜色上次修改时间
srvprvPreferredLocale	已保存的查询 / 搜索准则的列表
srvprvProcessXML	表示供应进程定义 （包括工作流程和供应操作）的 XML 文档
srvprvRequestDefName	与委托定义关联的供应请求定义名称。
srvprvRequestXML	表示初始请求表及其数据联结的 XML 文档
srvprvRevoke	一种标志，如果为 True，则指定供应请求定义支持撤消操作
srvprvStatus	指定受支持的值将包含的供应对象的状态
srvprvTaskGroups	用户担任任务管理员的组
srvprvUUID	入口小程序的唯一标识符
srvprvTaskManager	任务组的任务管理员
srvprvYahooIMAddress	Yahoo IM 地址

A.2 对象类纲要扩展

对象类名称	说明
srvprvAppConfig	**与自身 DirXML 驱动程序父级相连接的供应系统的应用程序配置对象的树枝**
srvprvAppDefs	用于初始化供应运行时环境 （如身份入口的主题）的配置对象的树枝
srvprvAssetRecipientAux	记录对用户的非 IT 资产供应情况
srvprvChoice	可以为特定特性指定的值、在查询中使用的值等值的枚举，这些值将用于身份入口小程序和其它万维网应用程序部件
srvprvChoiceDefs	目录提取层选择定义的树枝，将由身份入口小程序和万维网应用程序公开。
srvprvDelegateeAssignment	受委托者指派定义
srvprvDelegateeDefs	受委托者定义的树枝
srvprvDirectoryModel	目录提取层元级别对象的树枝，目录中选定的内容将由身份入口小程序和万维网应用程序公开
srvprvDirectoryModelConfig	运行时目录提取层配置参数
srvprvEntity	定义目录中已定义类的选定特性的视图，由身份入口小程序和其它万维网应用程序部件使用
srvprvEntityAux	标准对象类
srvprvEntityDefs	目录提取层实体定义的树枝，将由身份入口小程序和万维网应用程序公开
srvprvProxyAssignment	代理指派定义
srvprvProxyDefs	代理定义的树枝
srvprvRelationship	定义目录中对象之间的关系，以在身份入口小程序和其它万维网应用程序部件中使用
srvprvRelationshipDefs	目录提取层关系定义的树枝，将由身份入口小程序和万维网应用程序公开
srvprvRequest	公开一个要授予或撤消的可供应项目，包括定义工作流程和供应目标运行时方面的工作流程进程
srvprvRequestDefs	供应请求定义的树枝，可供应给万维网应用程序运行时的项目集
srvprvResource	定义要为供应履行操作 （授予或撤消）执行的目录指派集
srvprvResourceDefs	供应目标定义的树枝，包括设计时说明和任何模板或未使用的目标
srvprvService	说明如何从工作流程调用特定的万维网服务，这包括输入和返回值的规格
srvprvServiceDefs	服务定义对象的树枝，用于包装工作流程调用的 Web Services
srvprvTaskGroupAux	服务供应任务组

对象类名称	说明
srvprvAppConfig	**与自身 DirXML 驱动程序父级相连接的供应系统的应用程序配置对象的树枝**
srvprvTheme	主题对象
srvprvUserAux	服务供应用户实体
srvprvWebAppConfig	万维网应用程序配置对象
srvprvWorkflow	定义为获得供应操作的批准而需执行的活动 （包括遍历条件）网络
srvprvWorkflowDefs	工作流程对象的树枝，包括设计时说明和任何模板或未使用的流程
srvprvServiceDefs	服务定义对象的树枝，用于包装工作流程调用的 Web Services
srvprvStatus	指定受支持的值将包含的供应对象的状态
srvprvTaskGroupAux	服务供应任务组
srvprvTaskGroups	用户担任任务管理员的组
srvprvTaskManager	任务组的任务管理员
srvprvTheme	主题对象
srvprvUserAux	服务供应用户实体
srvprvWebAppConfig	万维网应用程序配置对象
srvprvWorkflow	定义为获得供应操作的批准而需执行的活动 （包括遍历条件）网络
srvprvWorkflowDefs	工作流程对象的树枝，包括设计时说明和任何模板或未使用的流程
srvprvYahooIMAddress	Yahoo IM 地址

A.3 LDIF 表示形式

下面给出了完整的纲要信息 （以 LDIF 格式），包括语法、树枝规则以及上面的摘要表中未显示的其它信息。这些信息可能会更改。

```
version: 1 # Copyright (c) 2004-2005 Unpublished Work of Novell, Inc.
All Rights # Reserved. # # THIS WORK IS AN UNPUBLISHED WORK AND
CONTAINS CONFIDENTIAL, # PROPRIETARY AND TRADE SECRET INFORMATION OF
NOVELL, INC. ACCESS TO # THIS WORK IS RESTRICTED TO (I) NOVELL, INC.
EMPLOYEES WHO HAVE A NEED # TO KNOW HOW TO PERFORM TASKS WITHIN THE
SCOPE OF THEIR ASSIGNMENTS AND # (II) ENTITIES OTHER THAN NOVELL, INC.
WHO HAVE ENTERED INTO #  APPROPRIATE LICENSE AGREEMENTS. NO PART OF
THIS WORK MAY BE USED, #  PRACTICED, PERFORMED, COPIED, DISTRIBUTED,
REVISED, MODIFIED, #  TRANSLATED, ABRIDGED, CONDENSED, EXPANDED,
COLLECTED, COMPILED, #  LINKED, RECAST, TRANSFORMED OR ADAPTED WITHOUT
THE PRIOR WRITTEN #  CONSENT OF NOVELL, INC. ANY USE OR EXPLOITATION OF
THIS WORK WITHOUT #  AUTHORIZATION COULD SUBJECT THE PERPETRATOR TO
```

```
CRIMINAL AND CIVIL #  LIABILITY. # # Base schema extensions for
SpitFire # # Last Modified: 6/27/05 (ek) # # See rfc2252 for
information on attribute syntax definitions #   String =
1.3.6.1.4.1.1466.115.121.1.15 #   Boolean =
1.3.6.1.4.1.1466.115.121.1.7 #   Octet String =
1.3.6.1.4.1.1466.115.121.1.40 #  DN = 1.3.6.1.4.1.1466.115.121.1.12 #
Case Exact String = 1.3.6.1.4.1.1466.115.121.1.26 #   Case Ignore List
= 2.16.840.1.113719.1.1.5.1.6 #   Case Ignore String =
1.3.6.1.4.1.1466.115.121.1.15 #   Stream =
1.3.6.1.4.1.1466.115.121.1.5 #   Time = 1.3.6.1.4.1.1466.115.121.1.24
# # OID registered for EPM: #   subarc "450" registered at: https://
wiki.innerweb.novell.com/wiki.phtml?title=OID_Registration #
attribute prefix: 2.16.840.1.113719.1.450.4.{3 digit unique per
attribute} #   object class prefix: 2.16.840.1.113719.1.450.6.{3 digit
unique number per class} #--------------------------------------------
----------------------------------------------------------------------
---------- #-- Framework Attributes #---------------------------------
----------------------------------------------------------------------
--------------------- dn: cn=schema changetype: modify add:
attributeTypes attributeTypes: ( 2.16.840.1.113719.1.450.4.127 NAME
'srvprvUUID' DESC 'Standard Attribute' SYNTAX
1.3.6.1.4.1.1466.115.121.1.26{64512} SINGLE-VALUE X-NDS_PUBLIC_READ
'1' X-NDS_NOT_SCHED_SYNC_IMMEDIATE '1' ) dn: cn=schema changetype:
modify add: objectClasses objectClasses: (
2.16.840.1.113719.1.450.6.127 NAME 'srvprvEntityAux' DESC 'Standard
ObjectClass' AUXILIARY MAY srvprvUUID X-NDS_NOT_CONTAINER '1' ) #-----
----------------------------------------------------------------------
------------------------------------------------- #-- User Attributes
#---------------------------------------------------------------------
------------------------------------------------------- dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.60 NAME 'srvprvHideUser' DESC 'Indicates if
a user is hidden during searches' SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
SINGLE-VALUE ) dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.61 NAME
'srvprvHideAttributes' DESC 'List of attributes a user is hiding from
other users' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 ) dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.62 NAME 'srvprvQueryList' DESC 'List of
saved query/search criteria' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE ) dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.63 NAME
'srvprvCapabilities1' DESC 'Place holder for classifying skills,
knowledge, references, etc.  Classifications are defined in the
application.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 ) dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.64 NAME 'srvprvCapabilities2' DESC 'Place
holder for classifying skills, knowledge, references, etc.
Classifications are defined in the application.' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 ) dn: cn=schema changetype: modify add:
attributeTypes attributeTypes: ( 2.16.840.1.113719.1.450.4.65 NAME
'srvprvCapabilities3' DESC 'Place holder for classifying skills,
knowledge, references, etc.  Classifications are defined in the
application.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 ) dn: cn=schema
```

```
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.66 NAME 'srvprvCapabilities4' DESC 'Place
holder for classifying skills, knowledge, references, etc.
Classifications are defined in the application.' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 ) dn: cn=schema changetype: modify add:
attributeTypes attributeTypes: ( 2.16.840.1.113719.1.450.4.67 NAME
'srvprvCapabilities5' DESC 'Place holder for classifying skills,
knowledge, references, etc.  Classifications are defined in the
application.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 ) dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.68 NAME 'srvprvIMAddress' DESC 'Key-value
pair of Instant messenger Addresses i.e. groupwise~jsmith' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 ) # This is temporary until we convert
the application to use the multi-value IM address (srvprvIMAddress)
above dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.69 NAME
'srvprvGroupwiseIMAddress' DESC 'Groupwise IM address' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) # This is temporary until
we convert the application to use the multi-value IM address
(srvprvIMAddress) above dn: cn=schema changetype: modify add:
attributeTypes attributeTypes: ( 2.16.840.1.113719.1.450.4.70 NAME
'srvprvYahooIMAddress' DESC 'Yahoo IM address' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) # This is temporary until
we convert the application to use the multi-value IM address
(srvprvIMAddress) above dn: cn=schema changetype: modify add:
attributeTypes attributeTypes: ( 2.16.840.1.113719.1.450.4.71 NAME
'srvprvAOLIMAddress' DESC 'AOL IM address' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.72 NAME 'srvprvActiveDelegatees' DESC 'The
active delegatees of a user' SYNTAX  2.16.840.1.113719.1.1.5.1.6 ) dn:
cn=schema changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.73 NAME 'srvprvActiveDelegators' DESC 'The
active delegators of a user' SYNTAX  2.16.840.1.113719.1.1.5.1.6 ) dn:
cn=schema changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.74 NAME 'srvprvIsTaskManager' DESC
'Indicates if user is a task group manager' SYNTAX
1.3.6.1.4.1.1466.115.121.1.7 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.75 NAME 'srvprvTaskGroups' DESC 'Groups for
which the user is a task manager' SYNTAX
1.3.6.1.4.1.1466.115.121.1.12 ) dn: cn=schema changetype: modify add:
attributeTypes attributeTypes: ( 2.16.840.1.113719.1.450.4.77 NAME
'srvprvPreferredLocale' DESC 'List of saved query/search criteria'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn: cn=schema
changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.128 NAME 'srvprvUserAux' DESC 'Service
provisioning user entity' AUXILIARY MAY ( srvprvHideUser $
srvprvHideAttributes $ srvprvQueryList $ srvprvCapabilities1 $
srvprvCapabilities2 $ srvprvCapabilities3 $ srvprvCapabilities4 $
srvprvCapabilities5 $ srvprvIMAddress $ srvprvGroupwiseIMAddress $
srvprvYahooIMAddress $  srvprvAOLIMAddress $ srvprvIsTaskManager $
srvprvTaskGroups $ srvprvActiveDelegatees $ srvprvActiveDelegators $
srvprvPreferredLocale) X-NDS_NOT_CONTAINER '1' ) dn: cn=schema
```

```
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.129 NAME 'srvprvTaskManager' DESC 'Task
manager of the task group' SYNTAX  1.3.6.1.4.1.1466.115.121.1.12 ) dn:
cn=schema changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.130 NAME 'srvprvTaskGroupAux' DESC 'Service
provisioning task group' AUXILIARY MAY ( srvprvTaskManager ) X-
NDS_NOT_CONTAINER '1' ) #-------------------------------------------
--------------------------------------------------------------------
--------- #-- Provisioning Attributes #------------------------------
--------------------------------------------------------------------
----------------------- dn: cn=schema changetype: modify add:
attributeTypes attributeTypes: ( 2.16.840.1.113719.1.450.4.100 NAME
'srvprvCategoryKey' DESC 'Associates a given Provisioning Request
Definition to a set of provisioning categories. Values are keys to a
srvprvChoice instance.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 ) dn:
cn=schema changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.101 NAME 'srvprvGrant' DESC 'Flag which if
true specifies that the Provisioning Request Definition supports a
Grant operation.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.7 SINGLE-VALUE )
dn: cn=schema changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.102 NAME 'srvprvRevoke' DESC 'Flag which if
true specifies that the Provisioning Request Definition supports a
Revoke operation.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.7 SINGLE-VALUE )
dn: cn=schema changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.103 NAME 'srvprvFlowStrategy' DESC
'Specifies the flow invocation strategy to be used for the Provisioning
Request Definition.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE
) dn: cn=schema changetype: modify add: attributeTypes attributeTypes:
( 2.16.840.1.113719.1.450.4.104 NAME 'srvprvLocalizedNames' DESC
'Provides set of localized display name strings for the provisioning
web applications, Designers and iManager.' SYNTAX
1.3.6.1.4.1.1466.115.121.1.26 ) dn: cn=schema changetype: modify add:
attributeTypes attributeTypes: ( 2.16.840.1.113719.1.450.4.105 NAME
'srvprvLocalizedDescrs' DESC 'Provides set of localized description
strings for the provisioning web applications, Designers and
iManager.' SYNTAX  1.3.6.1.4.1.1466.115.121.1.26 ) dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.106 NAME 'srvprvStatus' DESC 'Specifies the
status of the Provisioning Object. Supported values will include:
Inactive, Active, Template, and Retired.' SYNTAX
1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.107 NAME 'srvprvProcessXML' DESC 'XML
document representing a Provisioning process definition including
Workflow and Provisioning Action.' SYNTAX
1.3.6.1.4.1.1466.115.121.1.5 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.108 NAME 'srvprvEntityType' DESC 'Specifies
Directory Abstraction Layer Entity definition type: P-Public
definitions or S-System definitions.' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.109 NAME 'srvprvRequestXML' DESC 'XML
document representing the initial request form and its data bindings'
```

```
SYNTAX  1.3.6.1.4.1.1466.115.121.1.5 SINGLE-VALUE ) dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.110 NAME 'srvprvModified' DESC 'Flag to
indicate changes to definitions object instances in the directory
model container' SYNTAX  1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
dn: cn=schema changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.111 NAME 'srvprvEntitlementRef' DESC
'Reference to a DirXML-Entitlement' SYNTAX
1.3.6.1.4.1.1466.115.121.1.12 SINGLE-VALUE ) #-----------------------
---------------------------------------------------------------------
------------------------------ #-- Provisioning Configuration
Containers #---------------------------------------------------------
------------------------------------------------------------------ dn:
cn=schema changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.100 NAME 'srvprvAppConfig' DESC 'Container
for application configuration objects of the Provisioning System to
which its DirXML-Driver parent connects.' SUP top STRUCTURAL MUST ( cn
$ version ) MAY ( description ) X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT
( 'DirXML-Driver' ) ) dn: cn=schema changetype: modify add:
objectclasses objectClasses: ( 2.16.840.1.113719.1.450.6.101 NAME
'srvprvRequestDefs' DESC 'Container for Provisioning Request
Definitions, the set of provisionable items to the Web Application run-
time.' SUP top STRUCTURAL MUST ( cn ) MAY ( description ) X-NDS_NAMING
( 'cn' ) X-NDS_CONTAINMENT ( 'srvprvAppConfig' ) ) dn: cn=schema
changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.102 NAME 'srvprvWorkflowDefs' DESC
'Container for Workflow objects, including design-time descriptions
plus any template or unused flows.' SUP top STRUCTURAL MUST ( cn ) MAY
( description ) X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT (
'srvprvAppConfig' ) ) dn: cn=schema changetype: modify add:
objectclasses objectClasses: ( 2.16.840.1.113719.1.450.6.103 NAME
'srvprvResourceDefs' DESC 'Container for Provisioning Target
definitions, including design-time descriptions plus any template or
unused targets.' SUP top STRUCTURAL MUST ( cn ) MAY ( description ) X-
NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT ( 'srvprvAppConfig' ) ) dn:
cn=schema changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.104 NAME 'srvprvServiceDefs' DESC 'Container
for Service Definition objects, which wrap Web Services called by
Workflows.' SUP top STRUCTURAL MUST ( cn ) MAY ( description ) X-
NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT ( 'srvprvAppConfig' ) ) dn:
cn=schema changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.105 NAME 'srvprvDirectoryModel' DESC
'Container for Directory Abstraction Layer meta-level objects,
selected contents of the directory to be exposed by the Identity
Portlets and Web Applications.' SUP top STRUCTURAL MUST ( cn ) MAY (
description $ srvprvModified ) X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT
( 'srvprvAppConfig' ) ) dn: cn=schema changetype: modify add:
objectclasses objectClasses: ( 2.16.840.1.113719.1.450.6.106 NAME
'srvprvAppDefs' DESC 'Container for configuration objects used to
initialise the Provisioning run-time environment, such as themes for
the Identity Portal.' SUP top STRUCTURAL MUST ( cn ) MAY ( description
) X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT ( 'srvprvAppConfig' ) ) dn:
cn=schema changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.111 NAME 'srvprvEntityDefs' DESC 'Container
```

for Directory Abstraction Layer Entity defintions, to be exposed by the Identity Portlets and Web Applications.' SUP top STRUCTURAL MUST (cn) MAY (description) X-NDS_NAMING ('cn') X-NDS_CONTAINMENT ('srvprvDirectoryModel')) dn: cn=schema changetype: modify add: objectclasses objectClasses: (2.16.840.1.113719.1.450.6.112 NAME 'srvprvRelationshipDefs' DESC 'Container for Directory Abstraction Layer Relationship definitions, to be exposed by the Identity Portlets and Web Applications.' SUP top STRUCTURAL MUST (cn) MAY (description) X-NDS_NAMING ('cn') X-NDS_CONTAINMENT ('srvprvDirectoryModel')) dn: cn=schema changetype: modify add: objectclasses objectClasses: (2.16.840.1.113719.1.450.6.113 NAME 'srvprvChoiceDefs' DESC 'Container for Directory Abstraction Layer Choice definitions, to be exposed by the Identity Portlets and Web Applications.' SUP top STRUCTURAL MUST (cn) MAY (description) X-NDS_NAMING ('cn') X-NDS_CONTAINMENT ('srvprvDirectoryModel')) #### Provisioning Configuration Object Classes dn: cn=schema changetype: modify add: objectclasses objectClasses: (2.16.840.1.113719.1.450.6.107 NAME 'srvprvRequest' DESC 'Exposes one provisionable item to be granted or revoked, including the workflow process which defines the run-time aspects of the Workflow and Provisioning Target.' SUP top STRUCTURAL MUST (cn $ srvprvStatus $ srvprvFlowStrategy $ srvprvGrant $ srvprvRevoke $ srvprvCategoryKey $ srvprvLocalizedNames $ srvprvLocalizedDescrs) MAY (description $ srvprvEntitlementRef $ XmlData $ srvprvRequestXML $ srvprvProcessXML) X-NDS_NOT_CONTAINER '1' X-NDS_NAMING ('cn') X-NDS_CONTAINMENT ('srvprvRequestDefs')) dn: cn=schema changetype: modify add: objectclasses objectClasses: (2.16.840.1.113719.1.450.6.108 NAME 'srvprvWorkflow' DESC 'Defines the network of activites including traversal conditions to be executed in order to obtain approval for a provisioning action.' SUP top STRUCTURAL MUST (cn $ srvprvLocalizedNames $ srvprvLocalizedDescrs) MAY (description $ XmlData) X-NDS_NOT_CONTAINER '1' X-NDS_NAMING ('cn') X-NDS_CONTAINMENT ('srvprvWorkflowDefs')) dn: cn=schema changetype: modify add: objectclasses objectClasses: (2.16.840.1.113719.1.450.6.109 NAME 'srvprvResource' DESC 'Defines the set of directory assignments to execute for a provisioning fulfillment operation (either Grant or Revoke).' SUP top STRUCTURAL MUST (cn $ srvprvLocalizedNames $ srvprvLocalizedDescrs) MAY (description $ srvprvEntitlementRef $ XmlData) X-NDS_NOT_CONTAINER '1' X-NDS_NAMING ('cn') X-NDS_CONTAINMENT ('srvprvResourceDefs')) dn: cn=schema changetype: modify add: objectclasses objectClasses: (2.16.840.1.113719.1.450.6.110 NAME 'srvprvService' DESC 'Describes how to invoke a specific Web Service from an Workflow. This includes specification of input and return values.' SUP top STRUCTURAL MUST (cn) MAY (description $ XmlData) X-NDS_NOT_CONTAINER '1' X-NDS_NAMING ('cn') X-NDS_CONTAINMENT ('srvprvServiceDefs')) dn: cn=schema changetype: modify add: objectclasses objectClasses: (2.16.840.1.113719.1.450.6.114 NAME 'srvprvEntity' DESC 'Defines a view of selected attributes for defined classes in the directory, used by the Identity Portlets and other Web Application components.' SUP top STRUCTURAL MUST (cn $ srvprvEntityType) MAY (description $ XmlData) X-NDS_NOT_CONTAINER '1' X-NDS_NAMING ('cn') X-NDS_CONTAINMENT ('srvprvEntityDefs')) dn: cn=schema changetype: modify add: objectclasses objectClasses: (2.16.840.1.113719.1.450.6.115 NAME 'srvprvRelationship' DESC 'Defines relationships between objects in

```
the directory, for use in the Identity Portlets and other Web
Application components.' SUP top STRUCTURAL MUST ( cn ) MAY (
description $ XmlData ) X-NDS_NOT_CONTAINER '1' X-NDS_NAMING ( 'cn' )
X-NDS_CONTAINMENT ( 'srvprvRelationshipDefs' ) ) dn: cn=schema
changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.116 NAME 'srvprvChoice' DESC 'Enumeration of
values which can be assigned to a particular attribute, used in a
query, etc. for use in the Identity Portlets and other Web Application
components.' SUP top STRUCTURAL MUST ( cn ) MAY ( description $ XmlData
) X-NDS_NOT_CONTAINER '1' X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT (
'srvprvChoiceDefs' ) ) dn: cn=schema changetype: modify add:
objectclasses objectClasses: ( 2.16.840.113719.1.450.6.117 NAME
'srvprvDirectoryModelConfig' DESC 'Runtime Directory Abstraction Layer
configurarion parameters' SUP top STRUCTURAL MUST ( cn ) MAY (
description $ XmlData ) X-NDS_NOT_CONTAINER '1' X-NDS_NAMING ( 'cn' )
X-NDS_CONTAINMENT ( 'srvprvDirectoryModel' ) ) #### User Aux Classes
and Attributes dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.80 NAME 'srvprvAssetRef'
DESC 'Representation of the aggregate asset properties for a named
asset associated to a user via the srvprvAssetRecipientAux class.'
SYNTAX 2.16.840.1.113719.1.1.5.1.6 ) dn: cn=schema changetype: modify
add: objectclasses objectClasses: ( 2.16.840.1.113719.1.450.6.80 NAME
'srvprvAssetRecipientAux' DESC 'Records the provisioning of non-IT
assets on a user' AUXILIARY MAY ( srvprvAssetRef ) ) #----------------
----------------------------------------------------------------------
-------------------------------------- #-- Web Application Config
Class #--------------------------------------------------------------
-------------------------------------------------------------- dn:
cn=schema changetype: modify add: attributeTypes attributeTypes:
(2.16.840.1.113719.1.450.4.20 NAME 'srvprvDefaultTheme' DESC 'The
default theme' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn:
cn=schema changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.21 NAME 'srvprvWebAppConfig' DESC 'Web
Application Config Object' SUP top STRUCTURAL MUST (cn) MAY
(description $ srvprvDefaultTheme $ XmlData ) X-NDS_NOT_CONTAINER '1'
X-NDS_NAMING 'cn' X-NDS_CONTAINMENT ( 'srvprvAppDefs' ) ) #-----------
--------------------------------------------------------- ------------
------------------------------------------- #-- Theme Branding
Structural Class #---------------------------------------------------
----------------------------------------------------------------------
-- dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.21 NAME
'srvprvHeaderLogoImage' DESC 'Header Logo Primary Image' SYNTAX
1.3.6.1.4.1.1466.115.121.1.5 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.22 NAME 'srvprvHeaderLogoFile' DESC 'Header
Logo Primary Image File Name' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE ) dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.23 NAME
'srvprvHeaderLogoLastMod' DESC 'Header Logo Primary Last Modified'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.24 NAME 'srvprvHeaderLogo2Image' DESC
'Header Logo Secondary Image' SYNTAX 1.3.6.1.4.1.1466.115.121.1.5
```

```
SINGLE-VALUE ) dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.25 NAME
'srvprvHeaderLogo2File' DESC 'Header Logo Secondary Image File Name'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 | SINGLE-VALUE ) dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.26 NAME 'srvprvHeaderLogo2LastMod' DESC
'Header Logo Secondary Last Modified' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.27 NAME 'srvprvHeaderTextureImage' DESC
'Header Texture Image' SYNTAX 1.3.6.1.4.1.1466.115.121.1.5 SINGLE-
VALUE ) dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.28 NAME
'srvprvHeaderTextureFile' DESC 'Header Texture File Name' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.29 NAME 'srvprvHeaderTextureLastMod' DESC
'Header Texture Last Modified' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE ) dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.30 NAME
'srvprvHeaderFillerImage' DESC 'Header Filler Image' SYNTAX
1.3.6.1.4.1.1466.115.121.1.5 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.31 NAME 'srvprvHeaderFillerFile' DESC
'Header Filler File Name' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-
VALUE ) dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.32 NAME
'srvprvHeaderFillerLastMod' DESC 'Header Filler Last Modified' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.33 NAME 'srvprvLoginImage' DESC 'Login
Image' SYNTAX 1.3.6.1.4.1.1466.115.121.1.5 SINGLE-VALUE ) dn:
cn=schema changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.34 NAME 'srvprvLoginFile' DESC 'Login File
Name' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn:
cn=schema changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.35 NAME 'srvprvLoginLastMod' DESC 'Login
Last Modified' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn:
cn=schema changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.36 NAME 'srvprvLoginSmallImage' DESC 'Login
Small Image' SYNTAX 1.3.6.1.4.1.1466.115.121.1.5 SINGLE-VALUE ) dn:
cn=schema changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.37 NAME 'srvprvLoginSmallFile' DESC 'Login
Small File Name' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
dn: cn=schema changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.38 NAME 'srvprvLoginSmallLastMod' DESC
'Login Small Last Modified' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE ) dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.39 NAME 'srvprvNavColor'
DESC 'Navigation Color' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-
VALUE ) dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.40 NAME
'srvprvNavColorLastMod' DESC 'Navigation Color Last Modified' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn: cn=schema changetype:
```

```
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.41 NAME 'srvprvNavBckgrColor' DESC
'Navigation Background Color' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
SINGLE-VALUE ) dn: cn=schema changetype: modify add: attributeTypes
attributeTypes: ( 2.16.840.1.113719.1.450.4.42 NAME
'srvprvNavBckgrColorLastMod' DESC 'Navigation Background Color Last
Modified' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn:
cn=schema changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.20 NAME 'srvprvTheme' DESC 'Theme Object'
SUP top STRUCTURAL MUST (cn) MAY (description $ srvprvHeaderLogoImage
$ srvprvHeaderLogoFile $ srvprvHeaderLogoLastMod $
srvprvHeaderLogo2Image $ srvprvHeaderLogo2File $
srvprvHeaderLogo2LastMod $ srvprvHeaderTextureImage $
srvprvHeaderTextureFile $ srvprvHeaderTextureLastMod $
srvprvHeaderFillerImage $ srvprvHeaderFillerFile $
srvprvHeaderFillerLastMod $ srvprvLoginImage $ srvprvLoginFile $
srvprvLoginLastMod $ srvprvLoginSmallImage $ srvprvLoginSmallFile $
srvprvLoginSmallLastMod $ srvprvNavColor $ srvprvNavColorLastMod $
srvprvNavBckgrColor $ srvprvNavBckgrColorLastMod ) X-NDS_NOT_CONTAINER
'1' X-NDS_CONTAINMENT ( 'srvprvAppDefs' ) X-NDS_NAMING 'cn' ) #-------
----------------------------------------------------------------------
----------------------------------------------- #-- Attributes,
objects, and containers for Proxy, Delegatee and User availability, #-
----------------------------------------------------------------------
----------------------------------------------------- dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.120 NAME 'srvprvAssignFromUser' DESC 'User
subjects of a proxy or delegatee assignment' SYNTAX
1.3.6.1.4.1.1466.115.121.1.12 ) dn: cn=schema changetype: modify add:
attributeTypes attributeTypes: ( 2.16.840.1.113719.1.450.4.121 NAME
'srvprvAssignFromGroup' DESC 'Group subjects of a proxy or delegatee
assignment' SYNTAX  1.3.6.1.4.1.1466.115.121.1.12 ) dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.122 NAME 'srvprvAssignFromContainer' DESC
'Container subjects of a proxy or delegatee assignment' SYNTAX
1.3.6.1.4.1.1466.115.121.1.12 ) dn: cn=schema changetype: modify add:
attributeTypes attributeTypes: ( 2.16.840.1.113719.1.450.4.123 NAME
'srvprvAssignToUser' DESC 'The User targets of a proxy or delegatee
assignment' SYNTAX  1.3.6.1.4.1.1466.115.121.1.12 ) dn: cn=schema
changetype: modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.124 NAME 'srvprvAssignToRelationship' DESC
'A target relationship of a delegatee assignment' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.125 NAME 'srvprvAssignExpiration' DESC 'Time
at which a proxy or delegatee assignment expires' SYNTAX
1.3.6.1.4.1.1466.115.121.1.24 SINGLE-VALUE ) dn: cn=schema changetype:
modify add: attributeTypes attributeTypes: (
2.16.840.1.113719.1.450.4.126 NAME 'srvprvRequestDefName' DESC 'The
provisioning request definition name associated with a delegatee
definition.' SYNTAX  1.3.6.1.4.1.1466.115.121.1.12 ) dn: cn=schema
changetype: modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.120 NAME 'srvprvProxyDefs' DESC 'Container
for proxy definitions.' SUP top STRUCTURAL MUST ( cn ) MAY (
```

```
description ) X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT (
'srvprvAppConfig' ) ) dn: cn=schema changetype: modify add:
objectclasses objectClasses: ( 2.16.840.1.113719.1.450.6.121 NAME
'srvprvDelegateeDefs' DESC 'Container for delegatee definitions.' SUP
top STRUCTURAL MUST ( cn ) MAY ( description ) X-NDS_NAMING ( 'cn' ) X-
NDS_CONTAINMENT ( 'srvprvAppConfig' ) ) dn: cn=schema changetype:
modify add: objectclasses objectClasses: (
2.16.840.1.113719.1.450.6.122 NAME 'srvprvProxyAssignment' DESC 'Proxy
assignment definition' SUP top STRUCTURAL MUST ( cn $
srvprvAssignToUser ) MAY ( description $ srvprvAssignFromUser $
srvprvAssignFromGroup $ srvprvAssignFromContainer $
srvprvAssignExpiration ) X-NDS_NAMING ( 'cn' ) X-NDS_CONTAINMENT (
'srvprvProxyDefs' ) ) dn: cn=schema changetype: modify add:
objectclasses objectClasses: ( 2.16.840.1.113719.1.450.6.123 NAME
'srvprvDelegateeAssignment' DESC 'Delegatee assignment definition' SUP
top STRUCTURAL MUST cn MAY ( srvprvRequestDefName $ description $
srvprvAssignFromUser $ srvprvAssignFromGroup $
srvprvAssignFromContainer $ srvprvAssignToUser $
srvprvAssignToRelationship $ srvprvAssignExpiration ) X-NDS_NAMING (
'cn' ) X-NDS_CONTAINMENT ( 'srvprvDelegateeDefs' ) ) ############## DO
NOT DELETE THIS LINE ##################
#########################################################
```

配置应用程序存档

B

本附录介绍仅可通过编辑用户应用程序的 WAR 文件来配置的高级设置。包括以下主题：

- "关于用户应用程序 WAR" 在第 349 页
- "设置会话超时" 在第 349 页

B.1 关于用户应用程序 WAR

Identity Manager 用户应用程序封装成与 J2EE 兼容的万维网应用程序存档 (WAR) 文件。用户应用程序 WAR 文件包含 Java 类的集合以及控制应用程序运行时行为的 XML 文件。通常不应修改 WAR。但是，在极少数情况下，可能会发现有必要打开 WAR 文件并进行小规模的修改以控制应用程序的行为。

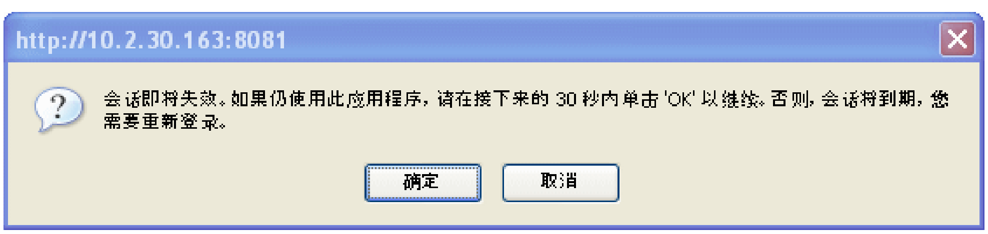
注释 : 本附录的剩余部分假定读者熟悉 J2EE 概念和过程。如果不确定如何在 WAR 文件内进行更改，请参阅 J2EE 文档。

B.2 设置会话超时

为了防止服务器上的非活动会话超载， Identity Manager 用户应用程序会暂停处于非活动状态时间过长的用户会话。默认超时间隔为 10 分钟。可通过编辑用户应用程序 WAR 文件的 WEB-INF 文件夹中的 *web.xml* 文件更改默认值。

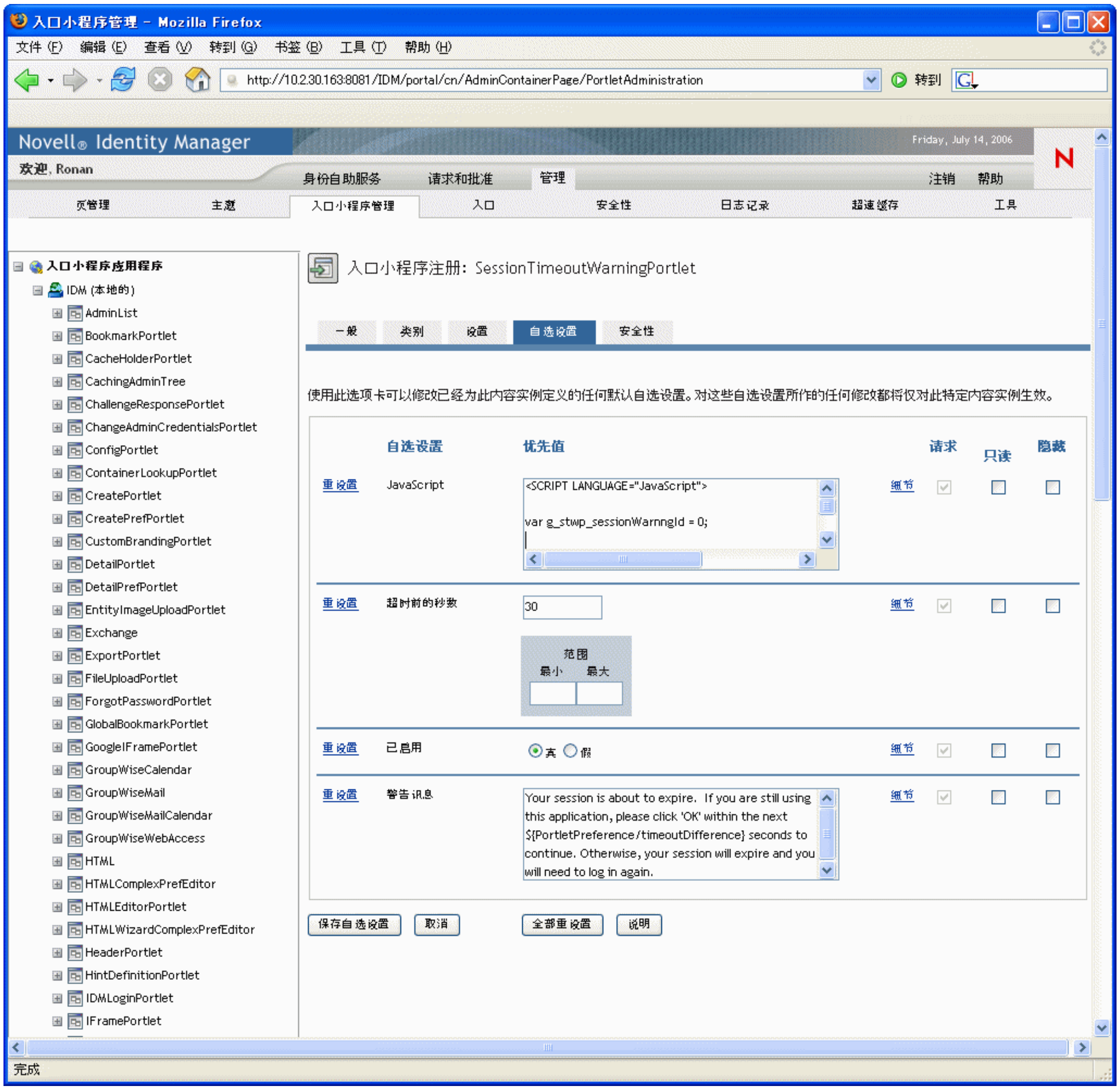
编辑会话超时间隔 WAR 中的 web.xml 文件有一个名为 <*session-timeout*> 的要素 （可在 <*session-config*> 要素下找到），它指定了会话在超时之前可处于不活动的时间。要设置会话超时间隔，请更改此要素的值。必须以分钟为单位指定此值。

控制警报讯息的行为 默认情况下，只要用户的会话即将超时， Identity Manager 用户应用程序就会显示一则警报讯息。



如果用户不单击 《确定》响应此讯息，则会话将超时。默认情况下，已启用警报讯息。如果愿意，可将其禁用。此外，还可以指定允许用户响应警报讯息的时间。

要控制警报讯息的行为，需要配置 *SessionTimeoutWarningPortlet*。为此，需要编辑入口小程序注册上的入口小程序自选设置，如下所示：



要指定允许用户响应警报讯息的时间，请编辑 《超时前的秒数》值。要完全禁用警报讯息，请单击 《启用》旁的 *False*。完成更改后，请单击 《保存自选设置》。